

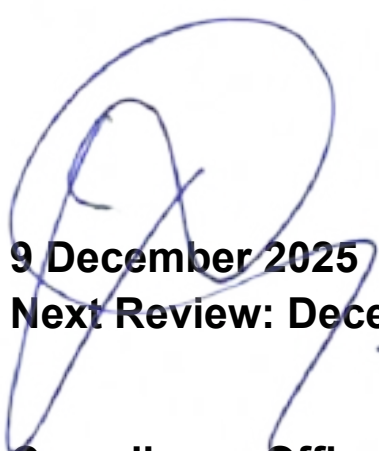


BY
KREVETKA B.V.

166108
Chuchubiweg 17, Cuacao

AML/CTF/CPF POLICY
2025/v2

APPROVED BY THE BOARD OF DIRECTORS



9 December 2025
Next Review: December 2026

Compliance Officer: Semen Klyuchyk /
compliance@krevetka.com

TABLE OF CONTENTS

1. Definitions	3
2. Statement of the Policy	5
3. Details of Online Gaming Landscape	6
4. Money Laundering, Terrorism Financing & Proliferation Financing	6
5. Integration of the National Risk Assessment	11
5.1. Customer Risk Assessment	14
5.2. Ongoing Monitoring	16
6. Risk-Based Approach	18
7. Customer Due Diligence & Enhanced Due Diligence	22
8. Customer Acceptance Policy	27
9. Transaction Monitoring	49
10. Politically Exposed Persons	51
11. Sanctions Policy	52
12. Suspicious & Unusual Activity & Transaction Reporting	61
12.1. Suspicious & Unusual Activity	63
12.2. Suspicious & Unusual Transactions	63
12.3. Timely Reporting	64
12.4. Confidentiality & Commitment to the Strong Reporting Culture	64
13. Compliance Officer	65
14. Senior Management	67
15. Employee Training & Screening	69
16. AML Compliance Audit	71
17. Regulatory Access & Cooperation	73
18. Internal Audit & Reporting	74
19. Record-Keeping	76
20. Appendices	77
Appendix 1: Customer Risk Calculator	78
Appendix 2 Employee Onboarding & Screening Form	80

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.

Suspicious Activity Report/Suspicious Transaction Report – **SAR/STR**

Counter Proliferation Financing – **CPF**

A senior management member who maintains independence from the games operations, responsible for deterrence and detection of ML/TF/CPF risks – **Compliance Officer**

The Financial Intelligence Unit Curacao, referred to in art. 2 of the Norut – **FIU**

Source of Funds/Wealth – **SOF/SOW**

Know Your Business – **KYB**

The United States – **US**

Office of Foreign Assets Control – **OFAC**

Ultimate Beneficial Owner – **UBO**

Know Your Customer – **KYC**

Customer Due Diligence – **CDD**

Counter Terrorism Financing – **CTF**

Enhanced Due Diligence – **EDD**

Politically Exposed Person – **PEP**

Anti-Money Laundering – **AML**

The Caribbean Financial Action Taskforce (an organization of 24 states of the Caribbean Basin, Central and South America) – **CFATF**

Board of Directors of the Company – **BoD**

The National Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen, P.B. 1993, no. 63) – **NOOGH**

The European Union – **EU**

The United Nations – **UN**

Financial Action Task Force – **FATF**

The United Kingdom – **UK**

2. 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. The policy is aligned with the new regulatory framework, effective as of January 2025 with full compliance as of April 10th, 2025.

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.

3. 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.

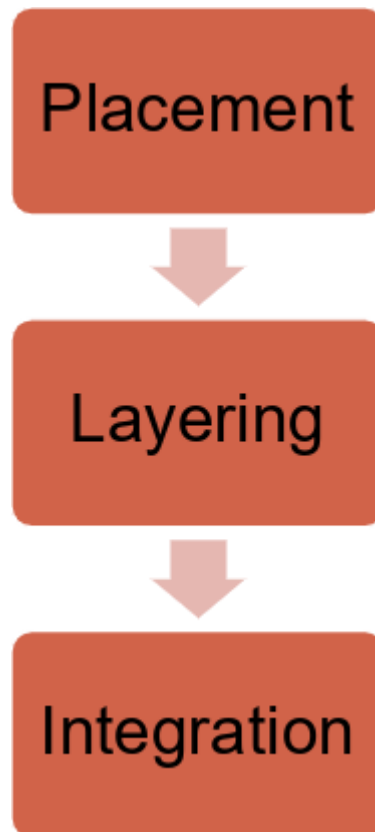
4. Money Laundering, Terrorism Financing & Proliferation Financing

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 withdrawals.

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.

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 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.

Proliferation Financing

Proliferation financing involves the provision of financial resources used to support the development, acquisition, or transfer of weapons of mass destruction (WMD), including nuclear, chemical, and biological weapons, as well as their associated delivery systems. These activities present a serious threat to international peace and security. Krevetka B.V., as a regulated online gaming operator licensed in Curaçao, is fully committed to mitigating any risk of involvement in proliferation financing, whether directly or indirectly. The company maintains a proactive compliance framework aligned with local legislation and international standards.

Sources of Proliferation Financing

Proliferation financing may arise from both legal and illegal sources, and Krevetka B.V. takes measures to identify and mitigate risk in both contexts.

Legitimate Origins Misused for Illicit Purposes

Funds that originate from seemingly lawful activities, such as business income, charitable contributions, or investments, can be diverted by proliferators to support WMD-related programs. To prevent such misuse, Krevetka B.V. closely reviews any transaction that involves high-risk jurisdictions or counterparties, particularly where there is a lack of transparency or legal justification.

Illicit Financial Activities

Funds derived from criminal conduct such as smuggling, fraud, or money laundering are often redirected toward proliferation objectives. Krevetka B.V. utilizes a multi-layered monitoring approach to detect unusual behavior or financial activity that may suggest an attempt to fund prohibited programs. Early intervention is central to the company's financial crime prevention efforts.

Funds may move through formal and informal channels, which are each subject to scrutiny.

- **Formal financial systems**, including banks and digital payment platforms, are vulnerable to exploitation through layering and complex transaction patterns. Krevetka B.V. leverages automated tools that flag inconsistent behavior in banking transactions, particularly where the source or use of funds is obscured.
- **Informal channels**, such as trade-based payment mechanisms or underground remittance networks, can operate beyond the scope of traditional oversight.

Transactions linked to regions with elevated proliferation risk or those involving goods with dual-use potential are subject to additional assessment to prevent regulatory evasion.

Monitoring and Detection Measures

Krevetka B.V. has implemented detection mechanisms to help identify potential instances of proliferation financing. These measures include the following risk indicators:

- **Trade-related anomalies**, especially where dual-use items are concerned. The company investigates transactions involving goods or services that may be suitable for both civilian and military applications, particularly when they involve jurisdictions or counterparties known for proliferation risk.
- **Business inconsistencies**, such as payments or patterns that diverge from the declared nature of the customer's activities. Unusual volumes, timing, or destinations of funds without a clear economic purpose are investigated.
- **Suspicious transaction behavior**, including frequent transfers to or from high-risk countries or sudden changes in financial activity, are flagged and subject to review in accordance with the company's risk-based approach.

Risk Mitigation and Compliance Actions

To prevent any exposure to proliferation financing, Krevetka B.V. relies on several key risk control tools:

Enhanced Customer Due Diligence

All customers operating in sectors, jurisdictions, or with transaction profiles that may raise concerns are subject to enhanced checks. These include verifying beneficial ownership, identifying links to high-risk industries, and assessing the legitimacy of the client's business operations.

Continuous Transaction Monitoring

The company's monitoring tools are calibrated to detect high-risk patterns such as unexplained cross-border payments or repeated transfers involving sanctioned entities. Each alert is reviewed by the Compliance Officer and escalated as needed.

Sanctions List Screening

Krevetka B.V. complies with all applicable sanctions regimes, including those enforced by the United Nations, European Union, and the United States Department of the Treasury's Office of Foreign Assets Control (OFAC). The company ensures that all customers, transactions, and counterparties are screened to avoid any prohibited dealings.

Regulatory and International Compliance

Krevetka B.V. observes and enforces all regulatory expectations under Curaçao's legal framework and global best practices, including the following:

- **Curaçao Requirements**

The company complies with the National Ordinance on the Penalization of Money Laundering (NOPML) and the National Ordinance on the Reporting of Unusual Transactions (NORUT), as required by the Curaçao Gaming Control Board (GCB). These rules mandate comprehensive internal controls to prevent abuse of the financial system.

- **FATF Recommendations**

The Financial Action Task Force (FATF) outlines global standards to prevent misuse of financial channels for WMD-related activities. Krevetka B.V. integrates these principles into its internal AML/CTF/CPF procedures.

- **UN, EU, and OFAC Sanctions**

Krevetka B.V. implements controls to prevent transactions involving sanctioned individuals or organizations that are identified by the UN, EU, or OFAC as being involved in proliferation programs. These include real-time alerts and automated blocking of flagged transactions or accounts.

Conclusion

Krevetka B.V. remains committed to global security efforts by ensuring that its services and platforms are never used to support the financing of weapons of mass destruction. Through its robust internal controls, customer due diligence processes, transaction monitoring systems, and strict sanctions compliance, the company actively mitigates risks associated with proliferation financing in full alignment with Curaçao regulations and international mandates.

5. Integration of the National Risk Assessment

Krevetka B.V. maintains a comprehensive and responsive AML/CTF/CPF compliance framework designed to protect its online gaming operations, financial activities, and digital infrastructure from misuse by individuals or entities engaged in money laundering, terrorism financing, or the funding of weapons proliferation. This framework is implemented in strict accordance with the laws and regulatory guidelines of Curaçao, including the requirements of the Curaçao Gaming Control Board (GCB), and is aligned with international standards such as those promoted by the Financial Action Task Force (FATF) and the Caribbean FATF (CFATF). All stakeholders, including employees, executives, third-party partners, and service providers, are expected to operate in line with this framework.

Governance and Oversight

The Board of Directors of Krevetka B.V. bears ultimate accountability for the oversight and enhancement of the AML/CTF/CPF compliance system. The Board ensures that appropriate human, technological, and financial resources are allocated to support effective risk mitigation tailored to the specific vulnerabilities of the remote gaming sector. Senior Management is responsible for translating Board strategy into operational practice and ensuring the Compliance Officer has full access to necessary tools, systems, data, and staff.

Role of the Compliance Officer and NRA Integration

The appointed Compliance Officer manages the execution of the compliance program and oversees daily activities such as customer due diligence (CDD/EDD), transaction monitoring, internal investigations, and the filing of reports with the Financial Intelligence Unit (FIU) of Curaçao. In accordance with AML Regulation III.1, the Compliance Officer ensures the company's internal controls are updated in response to changing regulatory landscapes and emerging financial crime risks.

Krevetka B.V. integrates insights from the most recent National Risk Assessment (NRA) issued by Curaçao authorities into its enterprise-wide risk framework. The Compliance Officer reviews and applies NRA findings across operational areas, reassessing customer risk ratings, evaluating jurisdictional exposure, scrutinizing new financial technologies, and adapting processes based on the identified typologies and threats.

Practical Application of NRA Insights

Findings from the NRA directly inform Krevetka B.V.'s Institutional Risk Assessment and its overall risk-based approach. Actions stemming from NRA integration include:

- Reinforcing identity verification and onboarding procedures.
- Recalibrating transaction monitoring thresholds and typologies.
- Applying stricter oversight to specific countries, client profiles, or payment platforms flagged as higher risk in the NRA.
- Deploying targeted alerts and real-time monitoring based on evolving threat indicators.

Whenever new threats or typologies are highlighted, the Compliance Officer evaluates the robustness of current measures and implements timely enhancements.

Risk-Based Due Diligence Measures

Krevetka B.V. enforces robust Know Your Customer (KYC) practices, especially before processing withdrawals or when customers exceed predetermined thresholds. Standard CDD procedures include identity validation, payment method checks, address

verification, and age confirmation. When elevated risks are detected, particularly those aligning with NRA-designated red flags, Enhanced Due Diligence (EDD) is applied, which may involve:

- Obtaining documented source of funds and wealth.
- Performing in-depth media and regulatory screening.
- Requiring management-level approval for account continuation.

EDD is mandatory for customers based in high-risk jurisdictions, politically exposed persons (PEPs), high-value players, and users exhibiting suspicious patterns or behavior.

Monitoring and Escalation

The company operates a dual-layer monitoring system, using both automated surveillance and manual review processes. Monitored activity includes:

- Frequency, volume, and methods of deposits.
- Unusual betting patterns or erratic gameplay.
- Use of tools designed to conceal user location (e.g., VPNs).
- Repeated exploitation of promotions or rapid account changes.

Alerts generated by the system are automatically forwarded to the Compliance Officer for investigation. Any transactions deemed suspicious are promptly reported to FIU Curaçao through the goAML platform, as required under AML Regulation IV.1 and the National Ordinance on the Reporting of Unusual Transactions (NORUT).

All staff are trained to identify and escalate suspicious behavior without delay. Strict internal protocols prohibit tipping-off or unauthorised disclosures, with violations treated as serious breaches subject to disciplinary action.

Record-Keeping and Training

Krevetka B.V. maintains a five-year minimum retention period for all compliance records, including KYC documentation, transaction logs, monitoring alerts, internal reviews, training records, and any documents related to the NRA.

All relevant employees undergo regular AML/CTF/CPF training, which includes specific modules on NRA outcomes and national vulnerabilities. Training is mandatory on an annual basis and is also refreshed following significant regulatory updates or the identification of new risks. The Compliance framework is reviewed each year and

updated where necessary to ensure continued alignment with the NRA and GCB guidance.

5.1. Customer Risk Assessment

Krevetka B.V. applies a structured, risk-based methodology to evaluate each customer's exposure to potential money laundering (ML), terrorist financing (TF), and proliferation financing (PF). This assessment is grounded in a client risk scoring model that examines various dimensions such as transactional behavior, geographic exposure, and other relevant risk indicators. The objective is to tailor the level of due diligence and ongoing monitoring based on the assessed risk level.

Risk Scoring Methodology

Each risk factor is assigned a weight, and the cumulative score determines the customer's risk classification. This score directly informs the appropriate due diligence measures and defines the level of internal approval required for onboarding and continued monitoring.

Risk Category	Score Range	Due Diligence Level	Approval Required
Low Risk	0 – 2	Standard Due Diligence	Client Services or Compliance Officer
Medium Risk	2 – 4	Standard Due Diligence	Client Services or Compliance Officer
High Risk	4 or above	Enhanced Due Diligence	Compliance Officer with annual review
Unacceptable Risk	Trigger-based	Rejected	Automatically declined

Customers assessed as low or medium risk undergo standard due diligence (SDD), including identity verification and routine monitoring. Clients falling within the high-risk category are subjected to enhanced due diligence (EDD), which involves collecting additional documentation, obtaining senior-level approvals, and scheduling periodic reassessments at least annually.

Any customer determined to pose an unacceptable risk such as those linked to sanctioned individuals or entities, or displaying critical red flags is denied access to the platform without exception.

This categorization process enables Krevetka B.V. to manage exposure effectively by aligning risk with appropriate compliance measures. The risk scoring framework is regularly updated to address evolving regulatory guidance and emerging typologies.

Screening and Risk Treatment

All clients, regardless of risk category, undergo screening for sanctions exposure, Politically Exposed Person (PEP) status, and adverse media at onboarding and on an ongoing basis. For details regarding the technical structure of the scoring model, see Appendix I.

Low-Risk Clients

Clients classified in this group are deemed to have a low likelihood of being involved in ML, TF, or PF. Nonetheless, due to the inherent risk of online gaming, simplified due diligence (SDD) is not applied. These clients undergo full standard due diligence as required by internal policy and regulatory standards.

Medium-Risk Clients

Clients falling into this category are flagged for moderate risk characteristics. They require close monitoring and must meet all standard Know Your Customer (KYC) requirements. Periodic profile reviews ensure that risk classifications remain accurate over time.

High-Risk Clients

High-risk clients are subject to enhanced scrutiny and require formal approval from the Compliance Officer. Typical indicators for this classification include:

- Use of opaque or complex legal structures.
- Transactional behavior that significantly deviates from known norms or expectations.
- Links to jurisdictions flagged as high-risk or sanctioned.
- Designation as a PEP, or association with a PEP.
- Elevated risk scores at onboarding or due to ongoing monitoring flags, such as frequent high-value deposits, adverse media mentions, or gambling behavior inconsistent with customer profile.

- Submitting falsified or unverifiable documentation.
- Engaging in transactions lacking clear legal or economic justification.
- Acting as intermediaries or custodians of funds on behalf of others.
- Reaching cumulative deposit levels that exceed predefined thresholds associated with high-risk patterns.

Unacceptable Client Profiles

Krevetka B.V. does not establish relationships with individuals or entities that:

- Are listed on domestic or international sanctions registers.
- Are suspected of involvement in ML, TF, or PF activities.
- Are under the legal gambling age of 18.
- Cannot substantiate the origin of funds or wealth with reasonable documentation.
- Exhibit behaviors consistent with known abuse patterns in the gaming sector.

The company's risk appetite is clearly defined, and relationships that exceed this threshold are not permitted. All assessments, classifications, and escalations are documented and maintained for review, with periodic updates based on internal findings and external developments.

5.2. Ongoing Monitoring

Krevetka B.V. maintains a continuous customer monitoring framework that aligns with its risk-based approach and meets its obligations under Curaçao's Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. This ongoing process ensures that client profiles remain accurate, due diligence information is kept current, and that any irregular or suspicious activities are identified and escalated without delay.

Continuous Screening Measures

The Compliance Department is responsible for regularly screening all clients against key external databases, including those related to Politically Exposed Persons (PEPs), international sanctions, and adverse media. In instances where screening results generate verified matches, the cases are escalated for further review and may lead to an event-driven reassessment of the client's profile.

Event-Driven Reviews

Krevetka B.V. initiates event-driven reviews in response to specific developments or risk signals. These reviews may result in a full refresh of the client's due diligence documentation and risk assessment. Common triggers for such reviews include:

- Discovery of new information that challenges the accuracy or completeness of previously collected customer data.
- Transactions or behaviors that deviate from the client's known profile or raise suspicion.
- Significant changes in the client's risk exposure or any new red flags.

Upon activation of an event-driven review, the client's risk classification is reassessed immediately and updated as necessary across all relevant records and compliance systems.

Periodic Risk-Based Reviews

In addition to reactive monitoring, Krevetka B.V. performs periodic reviews based on the customer's risk classification. These reviews aim to confirm that all client data remains current and that the assigned risk level remains appropriate:

- **High-Risk Clients** are reviewed annually. This includes re-verifying the residential address, reassessing the source of funds and wealth, performing updated adverse media screening, and evaluating all account activity during the review period.
- **Medium-Risk Clients** are subject to review every two years. During this process, the compliance team updates key due diligence information and assesses the client's financial behavior and gambling patterns.
- **Low-Risk Clients** are reviewed every three years, unless a trigger event calls for earlier action. Reviews include basic re-verification procedures and adverse media checks to confirm whether the client still qualifies for the low-risk designation.

Unscheduled reviews may also be initiated based on:

- Emergence of new risk factors or conflicting client information.
- Suspicious behavior, financial activity, or transaction patterns.

- Regulatory updates, changes in sectoral risk profiles, or requirements from supervisory bodies.

Adjustments Based on NRA Updates

Krevetka B.V. ensures that its monitoring practices remain aligned with the findings of the most recent National Risk Assessment (NRA) of Curaçao. If the NRA identifies new threats, vulnerabilities, or shifts in national priorities, the company promptly updates its internal procedures. This includes adjusting control mechanisms, modifying transaction monitoring thresholds, and refining the customer evaluation models to stay in step with national and international financial crime prevention standards.

By incorporating the latest risk intelligence and regulatory developments into its monitoring framework, Krevetka B.V. maintains a proactive and responsive compliance infrastructure capable of addressing evolving ML, TF, and PF threats.

6. Risk-Based Approach

Krevetka B.V. employs a thorough and structured risk-based methodology to identify, evaluate, and mitigate the potential misuse of its online gaming services for money laundering, terrorist financing, or proliferation financing. This approach aligns with the guidance issued by the Financial Action Task Force (FATF) and integrates both quantitative and qualitative assessments of threats, vulnerabilities, mitigation strategies, and their potential operational impact.

The company performs a comprehensive **Business Risk Assessment (BRA)** at least once per year, or when there are significant operational changes, the introduction of new products, or updates to the legal or regulatory landscape. The BRA is formally documented, reviewed, and approved by the Board of Directors, and updated as needed to account for new threats or regulatory developments.

Client Risk

Customers represent a key channel of exposure to financial crime. Krevetka B.V. evaluates individual client risk by examining behavioral patterns, financial complexity, and exposure to high-risk jurisdictions. Additional attention is given to Politically Exposed Persons (PEPs), clients with uncertain income sources, and those whose account behavior is inconsistent with declared financial status.

- **Low-risk clients** typically demonstrate stable and verifiable income, transparent account activity, and limited risk indicators.
- **High-risk clients** may engage in irregular or high-volume transactions, exhibit opaque financial backgrounds, or show links to sanctioned territories. These customers are subject to enhanced due diligence (EDD) and stricter monitoring

protocols.

Product, Service, and Transaction Risk

Certain offerings and transaction types inherently carry greater financial crime risk. This includes, but is not limited to, the use of cryptocurrencies, prepaid cards, digital wallets, and peer-to-peer functionalities, particularly where these may obscure the origin of funds.

To mitigate such risks, Krevetka B.V. applies a suite of tailored controls, including:

- Automated surveillance systems
- Transaction limits
- Alerts for abnormal betting behavior or sudden fund movements

These controls are calibrated to detect anomalies that fall outside the expected behavior for a given client profile.

Geographical Risk

Geographic location is a significant risk factor, particularly when clients are based in or connected to jurisdictions known for weak regulatory oversight, elevated corruption levels, or financial sanctions.

The company assesses jurisdictional risk using publicly available resources such as the FATF, Caribbean FATF (CFATF), OFAC, the European Commission, the US State Department, and Transparency International. Where a high-risk connection is identified, additional controls are enforced, such as:

- Mandatory EDD measures
- Manual transaction reviews
- Restrictions on account functionality

Distribution Channel Risk

The platform through which a customer engages with the company also informs the risk level. Krevetka B.V. recognizes that digital onboarding channels without in-person verification pose greater risks.

To manage this, the company uses:

- Biometric verification
- Multi-factor authentication
- Digital document validation tools

These controls ensure that all client onboarding, regardless of platform, meets the same regulatory standard and integrity expectations.

Technological Development Risk

Prior to implementing new technologies or significantly updating digital infrastructure, Krevetka B.V. carries out a formal, documented risk review. This process covers:

- Intended technology functionality
- Identified vulnerabilities
- Proposed risk mitigation strategies
- Residual risk assessment

This applies to the rollout of any new gaming platform, AI-based tool, payment interface, blockchain feature, or similar innovations. All findings are recorded and kept available for review by the Curaçao Gaming Control Board.

Sector-Specific Risk in Online Gaming

Krevetka B.V. acknowledges that the online gambling industry carries unique financial crime risks. Criminals may exploit the system through:

- High-speed betting
- Bonus abuse
- Structuring of winning claims to launder money

To combat this, the company:

- Restricts anonymous or unregulated payment instruments
- Requires use of licensed financial intermediaries

- Screens for red flags such as coordinated gameplay or rapid deposit/withdrawal cycles

Risk Mitigation and Monitoring

Risks identified through the BRA or during daily operations are addressed using specific countermeasures. These include:

- Collection of additional documentation
- Limitations on account functionality
- Application of enhanced monitoring protocols

Risk ratings are assigned to all clients and Payment Service Providers (PSPs) at onboarding and reviewed periodically or when relevant changes are observed. Ongoing monitoring includes:

- Sanctions status checks
- Negative news screening
- PEP identification and review

Documentation, Reporting, and Recordkeeping

Krevetka B.V. maintains a complete and secure record of:

- Risk classification decisions
- Due diligence actions
- Monitoring activities
- Outcomes of business risk reviews

All records are retained in accordance with legal retention obligations. Where suspicious activity is detected, reporting to the Financial Intelligence Unit (FIU) Curaçao is performed without delay. Disclosure of such reporting activities (tipping-off) is strictly prohibited.

Governance and Access Control

The company documents all risk assessments, including the BRA and Customer Risk Assessment (CRA), which contain detailed analyses of inherent and residual risks by

product, geography, and client type. These assessments are reviewed on a regular basis and made readily accessible to the Curaçao Gaming Control Board or any competent authority upon request.

7. Customer Due Diligence and Enhanced Due Diligence

Prior to onboarding any client, Krevetka B.V. is required to assess whether the individual presents any risks associated with money laundering (ML), terrorist financing (TF), or proliferation financing (PF). The objective is to safeguard the integrity of the platform and uphold regulatory compliance. The Customer Due Diligence (CDD) process forms a foundational component of the company's risk-based approach, enabling the early detection of red flags by reviewing client profiles, transactional behaviors, and their interaction with the company's services.

This process includes verifying a client's identity and age, gathering relevant financial and personal background information, assigning a risk score, and continuously observing behaviors for signs of suspicious activity. The company also makes use of publicly accessible information such as employment records, insolvency databases, social media, and property ownership records during its assessments.

In lower-risk situations, simplified due diligence may be considered. However, where risk factors are present, such as connections to high-risk countries or links to politically exposed persons (PEPs), enhanced due diligence becomes mandatory and is applied without exception.

Krevetka B.V. utilizes a structured risk scoring model that takes into account variables including geographic location, transaction patterns, service usage, and financial behavior. To strengthen its controls, the company incorporates advanced technology and trusted compliance tools, including AI-based monitoring, biometric verification, and third-party platforms such as LexisNexis and WorldCheck.

Anonymous or fictitious customer accounts are strictly prohibited. Every client must provide verifiable and authentic identity data. When potential irregularities are identified through the monitoring system, the Compliance Officer initiates appropriate steps, which may include reporting the incident to the Financial Intelligence Unit (FIU) and, where applicable, involving law enforcement authorities.

Clients are categorized into low, medium, or high-risk tiers under the Client Acceptance Policy (CAP), based on criteria such as transactional activity, geographic exposure, and source of funds. The policy outlines clear circumstances under which client relationships are declined or terminated due to unacceptable risk levels. More detail on these classifications is provided in Appendix IV.

When CDD Measures Are Applied

Krevetka B.V. enforces customer due diligence in the following scenarios:

- When a transaction equals or exceeds NAF 4,000, whether as a single transaction or a series of related transactions.
- When there is reasonable suspicion of criminal financial activity.
- When the legitimacy of prior identification documents is in doubt.
- When several smaller transactions are aggregated and surpass the NAF 4,000 threshold.
- When risk indicators trigger a higher level of scrutiny, regardless of transaction value.

The CDD process includes:

- Verifying customer identity through reliable, independent sources.
- Identifying and validating beneficial ownership for legal entities.
- Assessing corporate structures and exercising appropriate scrutiny.
- Continuously monitoring transactional patterns in line with the assigned risk profile.
- Verifying the source of funds when warranted by the risk level.
- Prioritizing internal reporting obligations over general verification procedures, especially in cases warranting FIU escalation.

Identity Verification and Data Collection

In order to confirm the legitimacy of each client's identity, Krevetka B.V. requires the following information:

- Full name
- Date and place of birth
- Residential address
- Nationality
- Identification number

Low-risk clients are required to submit only basic documentation. For high-risk clients, the company collects a broader range of supporting documents to facilitate in-depth evaluation of financial risk.

Accepted verification methods include:

- Government-issued identification documents (passport, national ID)
- Proof of address, such as utility bills or bank statements not older than six months
- Residential address confirmation via email, telephone, or postal verification
- Use of biometric checks, verification of payment methods, and analysis of IP location data

If the initial verification is insufficient, further measures may include video verification, facial recognition matching, or first deposit validation through an authorized financial institution.

In high-risk cases, clients must provide supporting documentation for source of funds and expected financial activity. For clients assigned medium or low risk, employment status or business activity details are required, with additional checks performed at the discretion of the Compliance Officer.

Timing of CDD Implementation

CDD is performed as early as possible in the customer lifecycle to reduce risk exposure. At the point of registration, clients are prompted to enter key identification details such as full name, date of birth, and address. These are verified against independent data sources. Any transactions meeting or exceeding the NAF 4,000 threshold, whether individually or cumulatively, trigger full due diligence.

In most cases, verification occurs during registration. However, if for any reason CDD is delayed, the following restrictions are imposed:

- Additional deposits or withdrawals are prohibited until verification is completed. Gameplay may continue with pre-existing funds.
- Withdrawal attempts result in a temporary account freeze.
- If verification remains incomplete after 30 days, the following actions are taken:
 - If suspicious activity is observed, a Suspicious Transaction Report (STR) is filed with the FIU.

- If no red flags are identified, funds are returned to the source of the initial deposit.
- If elevated risk persists, the account may be frozen or terminated in accordance with internal procedures.

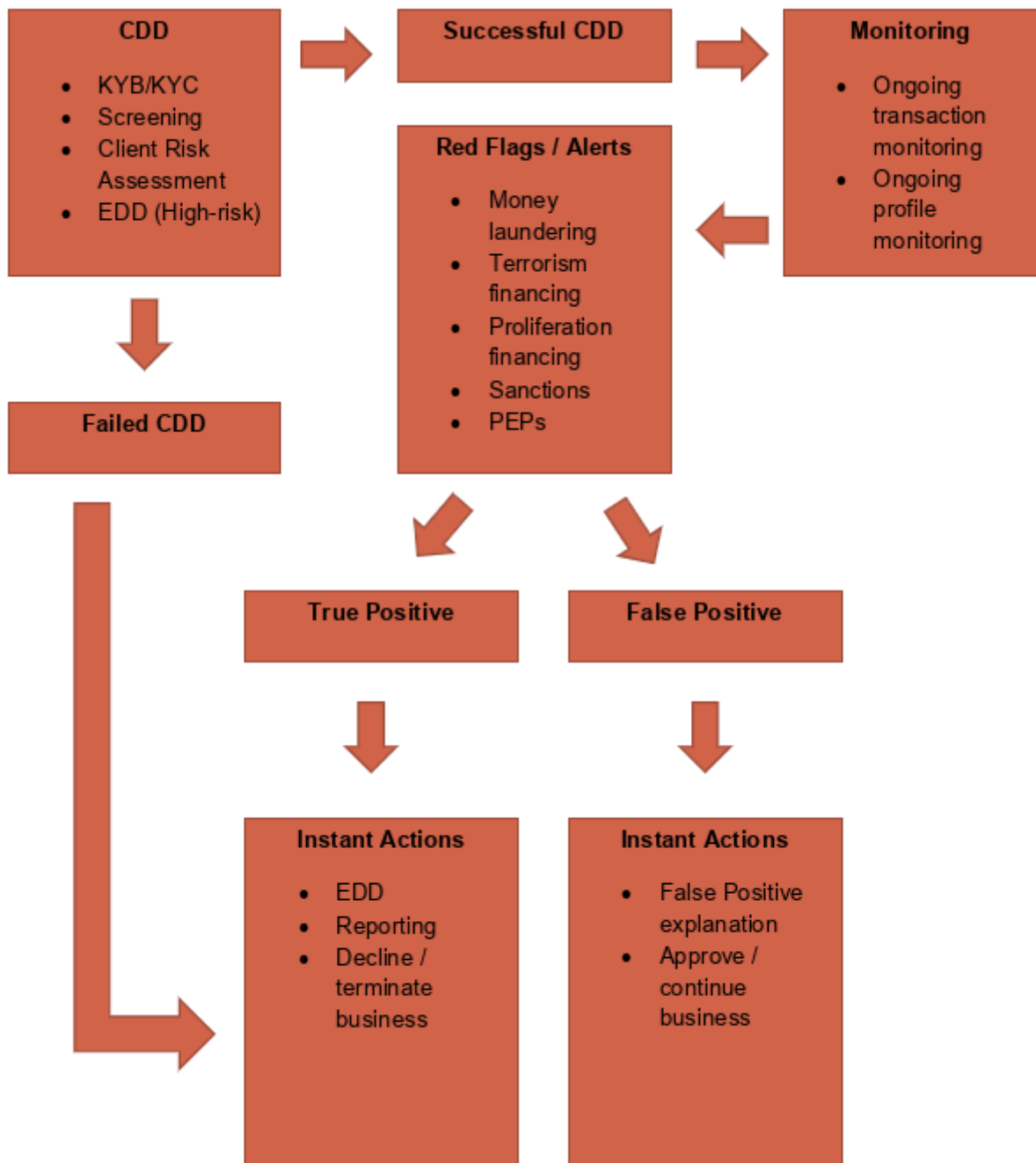
All CDD-related processes are conducted in a confidential manner. Tipping off is strictly prohibited, and employees are trained to maintain discretion at all times.

Monitoring continues throughout the customer relationship. Risk scores may be updated based on behavioral patterns, new information, or changes in regulatory requirements. CDD is reapplied in situations such as:

- Irregular or high-value financial activity
- Change in the client's country of residence
- Identification as a PEP
- Reaching NAF 4,000 in cumulative transactions again
- Legal or regulatory changes impacting due diligence thresholds

Legacy accounts created before current AML standards were implemented are prioritized for review, especially if classified as high-risk.

Where clients fail to complete the verification process or present unacceptable risks, the relationship is terminated. All such decisions are reviewed by the Compliance Officer. If any indication of ML, TF, or PF exists, an STR is submitted without delay. Documentation related to CDD and client relationships is retained for a minimum of five years following account closure.



Use of Third Parties in CDD

Krevetka B.V. may delegate certain CDD tasks to qualified third parties under specific and controlled conditions. Despite such reliance, ultimate responsibility remains with Krevetka B.V., and compliance with AML obligations cannot be outsourced.

Third-party providers must be:

- Regulated under comparable AML legislation

- Contractually bound to share records
- Subject to performance audits and compliance reviews

It is important to distinguish between third-party reliance and outsourcing. In reliance scenarios, the third party operates independently, while in outsourcing, they act under Krevetka B.V.'s direct control.

Before engaging a provider, the company evaluates the regulatory environment of the provider's jurisdiction, assesses historical performance, and ensures that data-sharing agreements are in place. Krevetka B.V. retains full control over final client acceptance decisions.

Beneficial Ownership and Control Verification

Krevetka B.V. takes all reasonable steps to identify and verify the ultimate beneficial owners (UBOs) of corporate clients. This process includes:

- Identifying individuals with direct or indirect ownership of 25 percent or more
- If no individual meets this threshold, determining who exercises control through voting rights, managerial roles, or legal arrangements
- Reviewing corporate structures involving layers, trusts, or nominee entities
- Requesting supporting documents such as shareholder lists, corporate registries, and organizational charts

Where ownership cannot be established, the senior-most executive is designated as the UBO, in accordance with international best practices.

All ownership data is verified using credible sources and retained securely. Krevetka B.V. does not enter into business relationships with clients that obstruct or delay the due diligence process.

8. Customer Acceptance Policy

Krevetka B.V. has established a Customer Acceptance Policy (CAP) to define the procedures, responsibilities, and internal controls governing the assessment and approval of individuals or entities seeking access to its licensed online gaming and betting platform. The primary objective of this policy is to safeguard the company from being exploited for illegal purposes, including money laundering, terrorist financing, proliferation financing, fraud, sanctions evasion, and other financial or regulatory misconduct. At the same time, the CAP ensures full compliance with the legal and regulatory framework applicable to gaming operations in Curaçao.

This policy is a fundamental element of Krevetka B.V.'s broader AML, CTF, and CPF compliance program. It aligns with the supervisory expectations of the Curaçao Gaming Control Board and incorporates internationally recognised standards, including those issued by the Financial Action Task Force (FATF), the European Union's AML Directives, and the principles endorsed by the Wolfsberg Group.

The CAP is grounded in Curaçao's legislative instruments such as the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

All personnel involved in customer onboarding and management, including directors, staff, contractors, and outsourced service providers, must adhere strictly to this policy. No client may deposit funds, place bets, or request withdrawals until all relevant verification procedures and acceptance requirements have been satisfied.

Scope and Applicability

This policy applies to all individuals and corporate entities attempting to register an account with Krevetka B.V., regardless of the onboarding channel. This includes registration through the company's website, mobile applications, affiliate partners, or third-party integrations.

The CAP applies throughout the entire lifecycle of the customer relationship, from initial registration until account closure or termination. It covers all products and services provided under Krevetka B.V.'s gaming licence OGL/2024/937/0857.

Eligibility and Access Criteria

Only clients who meet the legal and regulatory eligibility standards are permitted to use the company's services. All applicants must declare that they are at least eighteen years old, or older where local laws require it. The registration process requires clients to provide accurate and verifiable personal information, including full name, date and place of birth, nationality, and a valid residential address.

The company prohibits the onboarding of persons or entities based in or connected to jurisdictions that are subject to international sanctions, identified as high risk under internal policies, or otherwise restricted under Curaçao law. Sanctions screening is performed using global and regional databases such as those maintained by the United Nations, European Union, OFAC, OFSI, and other relevant authorities.

Clients may only use funds that originate from lawful and traceable sources. Where the customer presents an elevated risk, Krevetka B.V. may request further documentation to verify the origin of funds or wealth. The company also reserves the right to reject applicants with a history of abusive or fraudulent conduct, including chargeback abuse,

bonus misuse, or previous account closures due to self-exclusion or regulatory breaches.

Application of the Risk-Based Approach

Krevetka B.V. applies a risk-based methodology for customer onboarding and ongoing assessment. This enables the company to tailor its due diligence procedures according to the risk each client poses, based on their financial profile, transactional behaviour, jurisdiction, and methods of accessing services.

Each prospective customer is assigned a risk rating upon registration. Factors such as occupation, transaction patterns, geographic exposure, and prior gaming behaviour are analysed. Low-risk clients typically have stable income, consistent activity, and no red flags. High-risk clients include those with complex financial backgrounds, irregular deposits, or links to high-risk sectors or jurisdictions. PEPs, their family members, and close associates are automatically considered high risk.

Enhanced Due Diligence for High-Risk Clients

High-risk customers are subject to Enhanced Due Diligence (EDD). This includes rigorous identity verification, additional documentation requirements, and ongoing monitoring. Common EDD triggers include:

- Clients with unverifiable or inconsistent income who must provide tax documents or payslips.
- PEPs and related persons, requiring source of funds documentation, senior-level approval, and continuous oversight.
- Customers exhibiting gambling patterns inconsistent with their income.
- Sudden changes in transactional or gameplay behaviour.
- Use of proxies or intermediaries to manage financial transactions.
- Duplicate or linked accounts controlled by the same person.
- Large withdrawals without corresponding betting activity, particularly where third parties are involved.

When risk levels increase, the company responds with additional due diligence, restrictions on account functions, and heightened transaction review.

Geographic Risk Assessment

Clients are assessed based on their country of residence, the origin of their funds, or their transaction locations. Risk profiles are informed by data from FATF, CFATF, the European Commission, OFAC, the US State Department, and Transparency International.

Clients from sanctioned jurisdictions are automatically rejected. Those from high-risk regions may be permitted only after successful EDD and senior compliance approval. Affected customers undergo rigorous review, including documentation checks, verification of financial background, and intensified monitoring.

Risk Evaluation Workflow

The customer's risk profile is assessed through the following steps:

- Upon registration, country of residence and funding source are screened using real-time databases and watchlists.
- Clients from low-risk regions proceed under standard due diligence protocols.
- Clients from high-risk regions must undergo full EDD and obtain compliance clearance.
- Applications from sanctioned jurisdictions are rejected, and records of such rejections are maintained.
- Risk scores are reviewed dynamically and updated with new regulatory developments or intelligence.

Product and Transaction-Based Risk

Certain gaming features and payment tools present inherent risks due to their lack of transparency. These include:

- Peer-to-peer transfers or in-game tokens.
- Payment methods lacking user identification, such as prepaid cards and some cryptocurrencies.

Indicators of suspicious behaviour include:

- Large deposits followed by little or no gameplay, then withdrawal requests.
- Use of payment instruments not in the client's name.
- Repeated deposits and withdrawals without meaningful gaming activity.

All funds must come from verifiable legal sources. When concerns arise, clients must present credible documentation. Transactions suspected to involve criminal origins are reported to the FIU.

Payment methods with a degree of anonymity are treated as high risk and are subject to enhanced verification. Clients using wallets or financial services from poorly regulated jurisdictions must provide additional documents and may be subject to transaction limits or restrictions.

Transfers between user accounts are only permitted when clearly justified and pre-approved by the Compliance Officer. All such transactions are logged and monitored.

The use of multiple accounts is considered a red flag. Krevetka B.V. employs detection systems to identify linked profiles and prevent concealment of user behaviour. Unexplained changes to payment methods or banking details may also trigger reviews and enhanced controls.

Channel and Technology Risk

Remote onboarding introduces added exposure to identity fraud. To mitigate this, Krevetka B.V. uses secure onboarding methods, including:

- Biometric verification and document validation.
- IP and location checks.
- Multi-factor authentication.

Prior to implementing new technologies or payment options, the company conducts formal risk assessments. Any system or solution that could be exploited for illegal purposes is subject to approval and risk mitigation.

Technologies that facilitate customer anonymity require enhanced scrutiny. Verification steps may include real-time screening against PEP and sanctions databases, biometric tools, and additional due diligence.

Third-party involvement in onboarding or transaction processing increases risk, particularly when such parties are not regulated. Krevetka B.V. verifies their compliance credentials, checks their operational standards, and ensures transparency of all submitted information.

Risk Indicators

Krevetka B.V. applies a comprehensive framework of predefined risk indicators to evaluate the financial crime risk level associated with each customer. These indicators form an integral part of the company's risk-based approach and support the application of appropriate due diligence measures aligned with the customer's individual risk profile.

Core Risk Dimensions

The company's customer risk assessment is based on the following key categories:

- **Customer Risk Profile:** This includes factors such as multiple or irregular sources of income, status as a Politically Exposed Person (PEP), unusually high or inconsistent gambling expenditures, sudden behavioral shifts, the use of intermediaries, duplicate account registrations, unexplained fund redemptions, or connections to high-risk groups, including junket operations.
- **Product, Service, and Transaction Risk:** Indicators in this category include suspected use of criminally derived funds, use of anonymous or lightly regulated payment instruments, third-party account funding, frequent switching of payment methods, suspected use of false identity documents, or the concurrent use of multiple digital wallets.
- **Geographic Risk:** Applies to clients with links to jurisdictions that lack strong AML and CTF enforcement, exhibit high levels of corruption, are subject to international sanctions, or have been identified as associated with terrorist financing activity. Reference is made to assessments by FATF, CFATF, OFAC, and Transparency International's Corruption Perceptions Index (CPI).
- **Channel and Technology Risk:** Includes situations where clients access services through methods that reduce transparency, such as remote onboarding without adequate verification controls or the use of intermediaries not subject to regulatory oversight.

Risk Rating and Due Diligence Requirements

Krevetka B.V. uses an internal Risk Calculator that attributes weighted values to the indicators listed above. Based on the cumulative score, the customer is assigned a risk level and the corresponding due diligence requirements are applied as follows:

- **Low Risk:** Standard Customer Due Diligence (CDD) is sufficient. Documentation is limited to the legal minimum unless circumstances change.
- **Medium Risk:** Standard CDD is applied, supplemented by additional verification and closer monitoring.
- **High Risk:** Enhanced Due Diligence (EDD) is mandatory, including senior management approval before onboarding and increased monitoring throughout the customer lifecycle.

Risk Indicators Reference Table

Factor	Low Risk	Medium Risk	High Risk
Purpose of Account	Recreational or casual gambling	Consistent high-stakes or professional play	Bonus exploitation or use of platform for financial abuse
Source of Funds	Salary, pension, or other routine income	Business income, asset sales, inheritance	Unverifiable crypto, offshore funds, or unclear source of income
Source of Wealth	Employment, verified investments, inheritance	Sale of property or company	High-risk investments, offshore assets, or unverified origins
Transaction Frequency	Occasional	Weekly	Daily
Transaction Value (NAF)	Up to 1,000	1,000 to 4,000	Above 4,000
Incoming Payments	Bank cards or regular bank transfers	Prepaid cards or e-wallets	Cryptocurrency, third-party funding, deposits from high-risk locations
Outgoing Payments	Regular withdrawals or refunds	Bonus-linked withdrawals or frequent withdrawals	Crypto withdrawals, chargebacks, suspicious patterns
Gaming Behaviour	Consistent and moderate betting	High-stakes or prolonged sessions	Aggressive betting, collusion, multiple

			accounts, or suspicious activity
Payment Channels	Bank transfers	Verified e-wallets	Anonymous or unregulated payment tools
Adverse Media	No negative coverage	Unverified concerns	Verified criminal or illicit associations

Application of the Risk Indicators

These indicators are used by onboarding teams and compliance officers during customer onboarding, monitoring, and periodic reviews. Each risk factor is individually assessed and then collectively analyzed to determine the appropriate classification.

- Customers showing primarily low-risk traits are subject to standard due diligence.
- If a mixture of low- and medium-risk traits is present, the company applies additional verification and increases the monitoring level accordingly.
- If one or more high-risk indicators are detected, Enhanced Due Diligence (EDD) must be completed before any services are provided. Such cases also require review and approval by senior compliance personnel and may be subject to more frequent reassessment.

All risk classifications are periodically reviewed and adjusted based on behavioral changes, external alerts, or evolving regulatory requirements. This process ensures that Krevetka B.V. remains responsive to emerging threats and continues to fulfill its compliance obligations effectively.

Onboarding Procedures

Krevetka B.V. enforces a comprehensive and systematically documented onboarding process to ensure that only those customers who meet its regulatory, compliance, and internal risk tolerance criteria are granted access to its online gaming services. No player account is activated until all identification, verification, and sanctions screening steps have been satisfactorily completed.

Customer Registration and Identification

As part of the account registration process, all prospective clients must provide accurate and verifiable personal information, including:

- Full legal name
- Date and place of birth
- Nationality
- Residential address
- Official identification number (e.g., national ID or passport)

All customers are screened through automated systems that reference international sanctions lists and Politically Exposed Person (PEP) databases. Any potential matches are reviewed manually by trained compliance personnel to eliminate false positives and validate the legitimacy of the flagged data.

If a customer is initially assessed as high risk, Krevetka B.V. applies enhanced verification protocols. These may include, but are not limited to, the collection of documents confirming the origin of the customer's funds or broader wealth. Examples of acceptable supporting documentation include:

- Recent bank statements reflecting income deposits
- Payslips or income tax returns
- Financial statements for businesses or personal assets
- Contracts confirming the sale of assets
- Investment account statements

These checks reinforce the integrity of the onboarding process and ensure alignment with anti-financial crime measures.

Identity and Verification Requirements

This section applies to all individuals entering into a business relationship with Krevetka B.V., either directly or indirectly, including beneficial owners and authorized representatives.

Objectives of Document Verification

The company's verification efforts are intended to guard against:

- Document forgery

- Data manipulation
- Identity fraud
- The use of tampered or digitally altered files

All accepted identification documents must contain:

- The holder's full name
- Complete date of birth
- Document identification number
- Validity details (issue or expiry date)
- Photograph of the document holder
- Signature, where applicable

Documents must be:

- Valid for at least one month from the submission date
- Fully legible, undamaged, and complete

Upload and Validation Standards

Uploaded identification documents must adhere to the following specifications:

- Submitted in JPG, JPEG, PNG, or PDF format
- Full images of both sides (where applicable)
- At least 300 DPI or 100 KB file size
- Color images only
- All corners visible; no partial images or obstructing objects
- No digitally altered images or scans from screen captures
- Digital-only documents are not accepted unless explicitly authorized

Image Authenticity Measures

Krevetka B.V. uses automated systems to verify the integrity of uploaded documents through:

- Metadata analysis and file structure verification
- Review of source device signatures (camera or software)
- Risk scoring to detect image tampering
- Validation against standardized document templates
- Consistency checks on fonts, fields, and layout

All extracted data is cross-referenced with internal systems and external databases to ensure authenticity.

Proof of Address (PoA) Verification

For In-Person Clients

If the customer is onboarded face-to-face, the Money Laundering Compliance Officer (MLCO) reviews the original PoA document and stores a certified copy in compliance files.

For Remote Clients

For online account creation, the following steps apply:

- Upload of a PoA document issued within the past 90 days
- Image integrity and template validation
- Digital trust scoring and document pattern analysis
- Address verification using mapping services such as Google Maps or OpenStreetMap

Accepted PoA documents include:

- Utility bills (electricity, water, gas, internet)
- Bank or credit card statements

- Tax assessments or mortgage letters
- Residential lease agreements
- Voter or electoral registry certificates
- Employment letters or official government correspondence
- House deed documents

Alternative documents accepted if they include a full address:

- Passport
- National ID card
- Driving license
- EU residence permit

Non-acceptable documents:

- Mobile phone invoices
- Prepaid card statements
- Medical or insurance bills
- Documents listing only P.O. Box addresses
- Expired or outdated records (over 3 months old)

Note: A single document cannot be used to satisfy both ID and PoA requirements.

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

- **Source of Funds (SOF)** refers to the origin of specific deposits or payments made into the customer's gaming account.
- **Source of Wealth (SOW)** refers to the broader financial background of the customer.

To support SOF and SOW validation, Krevetka B.V. requires documentation corresponding to the declared source, such as:

Income Type	Documentation Examples
Employment income	Payslips, income tax returns, bank statements
Inheritance	Probate letters, wills, confirmation from legal professionals
Gifts/Donations	Notarized declarations, signed gift agreements
Savings	Bank savings statements showing history of accumulation
Government grants	Grant approval letters, benefit statements from relevant authorities
Dividends/Profits	Dividend statements, audited financial reports
Loans/Investments	Loan agreements, transfer receipts, investment confirmation documents
Property/Asset sales	Sales contracts, dealer confirmations, shipping records, or customs declarations

These documents must clearly demonstrate the legitimate connection between the customer and the transaction and ensure traceability and transparency in line with applicable AML and CTF regulations.

Ongoing Monitoring

Krevetka B.V. recognises that client onboarding is only the starting point of a broader compliance lifecycle. Continuous due diligence remains essential to ensure that each customer's conduct remains in line with the risk profile assigned during onboarding, and

to identify any developments that could indicate elevated exposure to financial crime risks.

To support this obligation, the company maintains automated monitoring systems capable of evaluating customer activity on a real-time basis. These systems are calibrated to flag any transactional or behavioural anomalies that could indicate misuse of the platform or attempts to circumvent anti-financial crime controls. Specific alert triggers include, but are not limited to:

- Transaction volumes or patterns that deviate from the established customer profile.
- The rapid movement of funds with minimal, inconsistent, or no gaming activity.
- Use of unfamiliar or irregular payment methods, or frequent switching between them.
- Behavioural patterns suggesting possible collusion, abuse of bonuses, or value transfer without economic justification.

All system-generated alerts are escalated to trained compliance officers who conduct manual assessments to determine whether further investigation, intervention, or escalation is required under internal protocols or reporting obligations.

In addition to real-time surveillance, Krevetka B.V. conducts risk-based periodic reviews of customer files to validate the currency and accuracy of due diligence data. These reviews help reassess whether the customer's assigned risk level remains appropriate or requires adjustment based on new information or behavioural developments. The following circumstances may prompt a reassessment or trigger a scheduled periodic review:

- A material change in the customer's residential status, such as relocation to or transactions from a jurisdiction classified as high risk.
- A significant increase in deposit frequency, betting turnover, or withdrawal volumes.
- A change in the source or nature of incoming payments, particularly when originating from unregulated providers or third parties.

Should any of these developments be observed, the customer's profile is re-evaluated. Where applicable, additional due diligence is applied, including enhanced documentation, approval from senior compliance officers, or temporary restrictions on account activity until verification is completed.

Prohibited Clients and Transaction Scenarios

To safeguard the platform from financial crime, regulatory non-compliance, and reputational damage, Krevetka B.V. enforces a clear prohibition on establishing or maintaining business relationships with certain client categories or executing particular types of transactions.

The company will not accept customers or facilitate transactions where any of the following conditions apply:

- The individual refuses to submit identification or verification documents necessary to establish an economic profile, unless a legitimate delay is formally justified.
- The client is subject to financial sanctions under the company's Sanctions Policy or included on watchlists from recognised authorities such as the United Nations, European Union, OFAC, OFSI, or national authorities of Curaçao.
- The client is linked to, or transacting through, a financial institution located in a jurisdiction without effective regulatory oversight, including shell banks or institutions that allow shell accounts.

Furthermore, the company shall not permit any customer to engage in business where there is a connection to, or suspicion of involvement in, any of the following:

- Acts of terrorism as defined in relevant European Union directives.
- Drug trafficking under the terms of the 1988 United Nations Convention.
- Organised crime syndicates or human trafficking operations.
- Fraud targeting the EU financial system, corruption involving state officials, or offences related to cybercrime, currency counterfeiting, or tax evasion.

Categories of Clients Subject to Immediate Rejection

Krevetka B.V. also enforces a strict exclusion policy for individuals or entities that present unacceptable risks or that do not comply with internal policies. Business relationships are automatically declined or suspended in the following cases:

- The client is anonymous, fails to complete identity verification within 30 days, or submits fraudulent or unverifiable documents.
- The client is using bearer instruments, operating in restricted sectors such as adult entertainment, or engaged in prohibited activities such as arms trafficking or

unlicensed virtual asset dealings.

- The client resides in, or transacts from, a jurisdiction prohibited by the company, including those subject to sanctions, extreme corruption, or lacking AML controls.
- The individual is under the minimum legal gambling age, or misrepresents their eligibility during registration.
- The customer is suspected of engaging in behaviour that includes account collusion, bonus abuse, gameplay manipulation, or identity fraud.

Krevetka B.V. also prohibits onboarding where the client's source of funds or source of wealth cannot be satisfactorily verified, or where it is suspected that the funds originate from criminal activity.

Prohibited Jurisdictions

In accordance with internal policies and regulatory obligations, Krevetka B.V. maintains a list of jurisdictions from which customer registrations and transactions are categorically blocked. These include both unrecognised territories and countries identified as high-risk, sanctioned, or incompatible with the company's compliance framework.

Unrecognised or disputed territories include:

Crimea, Donetsk, Luhansk, Republic of Abkhazia, Republic of South Ossetia, Nagorno Karabakh, Turkish Republic of Northern Cyprus, Palestine, Kosovo, Pridnestrovian Moldavian Republic, and Somaliland.

Prohibited countries include:

Australia, Belarus, Belize, Central African Republic, Cuba, Curaçao, Democratic Republic of Congo, Dutch West Indies (Aruba, Bonaire), France, Germany, Iran, Iraq, Lebanon, Libya, Mali, Netherlands, North Korea, Russia, Somalia, Sudan, Syria, United Kingdom, United States, and Yemen.

Customers from these jurisdictions are automatically declined during onboarding and any related transactions are blocked in real time. The rejection is logged, and records are retained to comply with the reporting obligations under Curaçao law.

Enhanced Due Diligence and Escalation Procedures

Where a customer presents elevated risks, Krevetka B.V. imposes Enhanced Due Diligence (EDD) obligations. These are mandatory for Politically Exposed Persons (PEPs), individuals linked to high-risk jurisdictions, or clients whose transactional

behaviour significantly exceeds what would be expected based on known financial indicators.

EDD includes a comprehensive review of the customer's financial background, verification of the origin of funds and wealth using reliable sources, and collection of supporting documentation such as:

- Financial statements, tax records, and employment confirmations.
- Asset sale contracts or verified investment portfolio details.
- Legal ownership documentation and company control structure verifications.

Customers subject to EDD are only approved upon review and authorisation by senior compliance staff. In certain high-risk cases, the final decision may rest with the Board of Directors. Upon acceptance, these clients are placed under intensified monitoring, which includes:

- Lower internal thresholds for triggering transaction reviews.
- Increased frequency of profile reassessments.
- Closer behavioural surveillance and automated alerting on high-risk activity.

This layered oversight ensures that Krevetka B.V. maintains strong control over high-risk exposures and acts in accordance with its legal and regulatory obligations under Curaçao's financial crime prevention laws.

Prohibited Categories of Customers

Krevetka B.V. maintains a strict prohibition policy against onboarding or continuing business relationships with individuals or entities that pose unacceptable legal, financial, regulatory, or reputational risks. The following categories of clients are explicitly excluded from accessing the company's online gaming services:

- Individuals using fictitious, anonymous, or misleading identities, or those who fail to complete full identity verification within the regulatory timeframe of 30 calendar days.
- Legal entities that are shell companies, non-transparent structures, or otherwise lack identifiable beneficial ownership or verifiable control.
- Any person or organisation included on relevant international or domestic sanctions lists, such as those published by the United Nations, European Union, United States (OFAC), United Kingdom (OFSI), or Curaçao authorities under the

Sanctions National Ordinance (SNO) or the Kingdom Sanction Act.

- Customers residing in or transacting from jurisdictions that are restricted under Krevetka B.V.'s internal policies or flagged as high-risk for money laundering, terrorist financing, or other financial crime.
- Underage individuals who have not reached the minimum legal gambling age as required in their country of residence and under Curaçao law.
- Clients with a history or suspicion of involvement in fraud, identity theft, abuse of bonus programs, or other illicit activities that could compromise the integrity of the gaming environment.
- Users funding their accounts through unverified third-party methods or anonymous sources, especially where no legitimate justification is provided.
- Any individual whose source of wealth or funds cannot be reasonably verified or is suspected of deriving from criminal activities.

Triggers for Immediate Rejection or Suspension

Krevetka B.V. reserves the right to immediately decline applications or suspend active accounts if any of the following risk triggers are identified during customer onboarding or throughout the business relationship:

Identity and Documentation Triggers

- Refusal or failure to provide Know Your Customer (KYC) documents, proof of address, or any other required verification within the applicable timeframe.
- Submission of counterfeit, tampered, or otherwise suspicious documentation, including signs of manipulation or forgery.
- Repeated non-responsiveness or failure to complete verification despite follow-up communications within the 30-day grace period.

AML/CTF/CPF Risk Indicators

- A match against Politically Exposed Person (PEP) or sanctions screening lists, where no suitable risk mitigation can be applied.
- Clear evidence or strong suspicion of involvement in money laundering, terrorist financing, proliferation financing, or comparable high-risk financial activities.

- Inability to establish a credible and legitimate source of funds or source of wealth after reasonable inquiry.

Behavioural and Transactional Red Flags

- Financial activity that is incompatible with the client's declared profile, such as frequent deposits or withdrawals without any verifiable gaming activity.
- Usage of multiple or linked accounts, third-party payments, or financial instruments not registered to the customer.
- Attempts to circumvent platform controls, obfuscate financial movements through intermediaries, or exploit system vulnerabilities.
- Observable patterns of gameplay manipulation, coordinated collusion, or repeated attempts to benefit from promotions inappropriately.

Termination of Customer Relationships

Krevetka B.V. may unilaterally suspend or terminate any customer relationship where such action is necessary to uphold legal compliance, safeguard the platform's integrity, or address unacceptable risk. Termination decisions are executed in accordance with the company's internal policies, risk assessments, and applicable legal provisions.

Common grounds for termination include:

- Failure by the customer to submit required KYC, verification, or source of funds documentation within the prescribed timeframe.
- Credible suspicion or evidence of the customer's involvement in activities related to money laundering, terrorism financing, or proliferation financing.
- Violation of applicable laws, Curaçao's gaming regulations, or breach of the Responsible Gambling Policy.
- Registration or activity from jurisdictions explicitly prohibited or sanctioned under company policy.
- Submission of false, incomplete, or deliberately misleading registration or verification information.
- The customer's financial behavior cannot be reconciled with their declared background, and no supporting documentation is provided.

- Confirmation or suspicion of the customer's status as a PEP where the associated risk cannot be adequately mitigated.
- Confirmed cases of promotional abuse, use of fake identities, collusion with other users, or engagement in unauthorised gambling practices.
- Use of payment methods registered under third parties without transparent explanation or authorisation.
- Evidence of chip dumping, staged betting, or substantial withdrawals with no meaningful gameplay history.
- Verification that the customer is underage at the time of registration or gameplay.

When termination is initiated on grounds involving potential financial crime, Krevetka B.V. immediately files a Suspicious Transaction Report (STR) with the Financial Intelligence Unit (FIU) Curaçao in compliance with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Residual balances, if not subject to freezing or seizure orders, are returned to the original funding source, and the account is closed with all actions properly documented.

Records of termination decisions, including justifications, associated evidence, and follow-up actions, are retained in accordance with the company's recordkeeping obligations and held securely for a minimum of five years.

Legal and Regulatory Compliance in Curaçao

The Customer Acceptance Policy represents a foundational element of Krevetka B.V.'s broader Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing program. This policy is fully aligned with Curaçao's legal and regulatory framework, which includes:

- The National Ordinance on Identification when Rendering Services (NOIS)
- The National Ordinance on the Reporting of Unusual Transactions (NORUT)
- The Sanctions National Ordinance (SNO)
- The Kingdom Sanction Act
- The National Ordinance on Games of Chance (LOK)

These legal instruments are integrated into the company's operational protocols and client management processes. The CAP's implementation extends across the customer

lifecycle, including onboarding, ongoing due diligence, periodic reviews, and exit procedures.

All personnel involved in customer-facing, onboarding, verification, and compliance tasks are required to complete dedicated training on regulatory requirements, internal procedures, and risk indicators. The aim is to ensure that all relevant teams are equipped to detect elevated risks, escalate problematic cases, and apply the company's risk-based controls consistently.

To ensure accountability and continuous improvement, Krevetka B.V. arranges independent audits of its customer acceptance framework at least once per calendar year. These audits assess compliance with KYC, screening, and EDD procedures. Findings are reported to the Board of Directors and any deficiencies identified are addressed through time-bound corrective action plans.

Integration with Responsible Gambling Framework

Krevetka B.V. ensures that its Customer Acceptance Policy is closely integrated with its Responsible Gambling Policy, recognizing the importance of protecting individuals from gambling-related harm as a fundamental compliance and ethical obligation.

When customer activity indicates potential harm, such as frequent deposits that appear inconsistent with the individual's financial means or extended periods of gameplay, the company initiates timely intervention. Depending on the situation, the following actions may be taken:

- Application of deposit or loss limits
- Temporary restriction of access to specific services
- Temporary suspension of the account
- Full account lockout to safeguard the customer

Self-exclusion requests are implemented without delay and applied across all associated accounts held by the customer, ensuring that the restriction cannot be bypassed across platforms. These self-exclusion settings remain in force for the full duration requested by the customer or as required by applicable law.

Employees in frontline or customer support roles receive specific training to help them identify early warning signs of problematic gambling behavior. This training is built into both the onboarding process and continuous monitoring, enabling staff to initiate timely support and refer customers for further assistance when needed.

Policy Review and Oversight

The Customer Acceptance Policy is reviewed at least once per year to ensure that it remains fully aligned with applicable laws, regulatory requirements, and internal business developments. The purpose of the review is to:

- Maintain compliance with the regulatory and legislative obligations applicable in Curaçao
- Reflect updates in the company's risk profile, operational scope, or business model
- Integrate risk insights gained through internal assessments or regulatory guidance
- Adapt to evolving international best practices in AML, CTF, CPF, and onboarding compliance

The Compliance Officer leads the review process, prepares any proposed amendments, and submits them for approval to the Board of Directors. Once approved, the updated policy is circulated internally, and relevant staff are trained on the new provisions to ensure proper implementation.

Record Retention and Data Protection

Krevetka B.V. securely retains all records related to customer acceptance and verification for a minimum of five years following the termination of the business relationship, in accordance with legal retention requirements.

The types of records maintained include:

- Identity verification and registration documents
- Proof of residential address
- Documentation supporting source of funds and wealth
- Risk assessments and due diligence records
- Transaction monitoring alerts and compliance investigations
- Records related to Enhanced Due Diligence (EDD)
- Account restriction, suspension, and closure documentation

All records are stored in encrypted format with access limited strictly to authorized compliance personnel. Access logs are maintained and regularly audited to ensure

compliance with data protection policies. Krevetka B.V. is fully committed to protecting customer data in accordance with relevant data privacy laws and industry standards.

9. Transaction Monitoring

Krevetka B.V. acknowledges that effective transaction monitoring is a fundamental element of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) control framework. Given the fast-paced and high-volume nature of the online betting and gaming environment, the risk of exploitation for illicit purposes remains significant. As a result, the Company operates a comprehensive, technology-driven transaction monitoring system capable of identifying, assessing, and responding to potentially suspicious activity in real time.

Compliance with Curaçao Regulatory Requirements

Krevetka B.V. maintains a monitoring infrastructure fully aligned with the legal and regulatory standards established under Curaçao law, including the National Ordinance on the Reporting of Unusual Transactions (NORUT) and the Sanctions National Ordinance (SNO). The design and functionality of this framework reflect the supervisory expectations of the Financial Intelligence Unit (FIU Curaçao) and support ongoing compliance with all mandatory reporting and escalation obligations.

Monitoring Architecture and System Design

The Company employs a real-time transaction monitoring platform that integrates both automated detection algorithms and manual compliance oversight. This dual-layered system uses machine learning, behavioural pattern analysis, and risk-based flagging mechanisms to identify transactions that may present financial crime risks. Alerts are automatically triggered when pre-set thresholds are breached or when anomalies are detected relative to the customer's known profile. These alerts are escalated to the Compliance Department for further evaluation and, where warranted, formal investigation.

Key indicators of suspicious activity include but are not limited to:

- High-value or inconsistent deposits not in line with customer risk profiles
- Use of multiple payment instruments, especially those considered unregulated or anonymous
- Deposit and withdrawal cycles with little or no genuine gameplay
- Movement of funds between related or suspected linked accounts
- Frequent transactions originating from or directed to jurisdictions known for banking secrecy or poor AML enforcement

Risk-Based Configuration and Transaction Scoring

All transactional activity is assessed against risk parameters calibrated to account for individual customer profiles, transaction values, velocity, and origin of funds. Transactions are assigned a risk score, and alerts are generated when those scores surpass defined thresholds.

Standard triggers include:

- Any single transaction of NAF 4,000 or more, or linked transactions cumulatively reaching this threshold
- Irregular or excessive deposit/withdrawal patterns
- Activity inconsistent with declared income or verified Source of Funds (SOF)
- IP address mismatches and geolocation flags indicating possible access from high-risk or restricted regions

When the cumulative transaction amount equals or exceeds NAF 4,000, full Customer Due Diligence (CDD) is initiated, including customer re-verification where required, regardless of whether the total was reached via multiple smaller transactions.

Monitoring Techniques and Data Analysis

Krevetka B.V. applies a range of data analysis methods to ensure effective oversight, including:

- **Geolocation filtering** – restricting access from prohibited or high-risk jurisdictions
- **IP address correlation** – detecting suspicious login patterns or duplicate accounts
- **Velocity checks** – identifying abnormally rapid deposit or withdrawal cycles
- **SOF validation** – cross-checking declared income with transaction behaviour
- **Behavioural profiling** – flagging sharp deviations from historical betting or gameplay activity

The system continuously processes data streams such as deposit methods, average stake values, session duration, betting trends, win/loss history, and device usage to establish behavioural baselines and detect irregularities.

Internal Escalation and Regulatory Reporting

Where a transaction or series of activities triggers suspicion, an internal Suspicious Activity Report (SAR) is compiled and submitted to the AML/CTF Officer for review. If deemed reportable, the incident is escalated to the FIU Curaçao under the statutory requirements of the NORUT framework. The Company ensures that all alerts, supporting documentation, and decisions taken are fully documented, time-stamped, and retained for regulatory inspection or audit.

If the CDD or Enhanced Due Diligence (EDD) process cannot be successfully completed due to customer refusal or insufficient documentation, the Company proceeds to freeze the account and terminate the business relationship. In such cases, any remaining funds are returned to the original source of payment unless regulatory holds, seizure orders, or enforcement actions apply.

10. Politically Exposed Persons

At Krevetka B.V., Enhanced Due Diligence (EDD) is a critical part of the compliance framework, particularly when assessing individuals who may present a higher financial crime risk. EDD ensures deeper scrutiny of customer background and transactional behavior to identify and mitigate potential exposure to money laundering, fraud, and related criminal conduct.

One of the key categories of high-risk customers includes those classified as Politically Exposed Persons (PEPs). A PEP is defined as an individual who currently holds, or has recently held, a prominent public position. This includes, but is not limited to, heads of state, senior politicians, members of parliament, judicial or military officials, executives of state-owned enterprises, and high-ranking officials of international organisations. In addition, close family members and known associates of PEPs are treated with the same elevated level of scrutiny.

Whenever a customer is identified as a PEP, Krevetka B.V. applies strict onboarding controls. These include a comprehensive risk assessment and full verification of the customer's source of wealth and source of funds. No account may be opened or operated without explicit written approval from senior management. This ensures that decision-making is handled at the appropriate level of authority and that potential risks are fully understood before proceeding.

All confirmed PEPs are recorded in an internal register maintained by the Compliance Officer. This register includes details of the risk evaluation and any mitigating measures applied. It is reviewed and monitored periodically and on an ongoing basis to ensure it remains accurate and reflects any relevant updates in the customer's risk profile.

These procedures form part of Krevetka B.V.'s broader risk-based approach and are designed to comply with Curaçao's AML, CTF, and CPF regulatory requirements. By applying heightened controls to PEP relationships, the company protects its platform

from being misused for illicit purposes while demonstrating strong regulatory adherence and ethical conduct.

11. Sanctions Policy

Krevetka B.V. is fully committed to upholding all legal requirements related to international sanctions. This policy outlines the procedures and internal controls the company uses to identify, prevent, and mitigate risks arising from dealings with sanctioned individuals, entities, or territories. Sanctions are imposed by national and international authorities to support foreign policy, national security, and the enforcement of international standards.

Sanctions may take various forms depending on the issuing body and its objectives. The main categories include:

- **Comprehensive Sanctions:** These impose a broad prohibition on nearly all forms of economic engagement with particular countries or regions, such as the Crimea territory. They are intended to create economic pressure by limiting access to international markets and resources.
- **Regime-Based Sanctions:** These target political leaders, institutions, or entities involved in or associated with human rights violations, corruption, or destabilising conduct. Measures often include restrictions on trade and asset freezes.
- **Sectoral Sanctions:** Applied to specific sectors of a country's economy such as energy, defense, or finance, these sanctions restrict particular types of transactions while allowing limited commercial activity.
- **Debt and Equity Sanctions:** These limit financial market access by prohibiting involvement in specific forms of financing or capital transactions, particularly for state-linked or strategic entities.
- **Conduct-Based Sanctions:** These target persons or entities connected to activities such as terrorism, cybercrime, arms trafficking, organized crime, or corruption. Designation is based on behaviour rather than nationality or jurisdiction.

These sanction categories often overlap, and a single sanctions regime may contain features from more than one category.

Applicable Sanctions Frameworks

Due to the global nature of its services, Krevetka B.V. adheres to a variety of international sanctions regimes. These include:

United Nations (UN)

The company respects the sanctions imposed by the UN Security Council under Chapter VII of the UN Charter. These are legally binding on all member states and are incorporated into the company's compliance framework.

European Union (EU)

EU sanctions apply to:

- Individuals and companies in the EU
- EU nationals worldwide
- Businesses incorporated in the EU and their overseas branches
- All activities with an EU connection
- Aircrafts or ships under EU jurisdiction

Krevetka B.V. complies with all relevant EU sanctions across its operations, regardless of location.

United Kingdom (UK)

UK sanctions cover:

- Activities within the UK and its territorial waters
- UK nationals and companies, including foreign branches
- Any business conducted in full or in part within the UK

UK sanctions are followed unless they conflict with prevailing EU laws.

United States (US)

US sanctions include:

- **Primary sanctions**, which apply to US persons, entities, and their foreign subsidiaries or controlled businesses.
- **Secondary sanctions**, which apply to non-US parties that engage in activities the US deems contrary to its foreign policy interests, particularly in countries like

Iran, China, or Russia.

Krevetka B.V. applies US sanctions to the extent they do not conflict with EU regulations or local law. Where conflicts arise, such as with the EU Blocking Statute (Council Regulation (EC) No 2271/96), the Compliance Officer refers the issue to the Directors and Board for a decision.

Policy Commitments

Krevetka B.V. undertakes to:

- Block or freeze accounts when mandated by sanctions
- Prevent any transactions with sanctioned countries, individuals, or companies unless explicitly permitted
- End relationships with sanctioned parties, even if the jurisdiction allows continuation. Where local law prohibits such termination, the matter is escalated to the Board
- Detect and stop attempts to circumvent sanctions through misrepresentation or structuring

Breach Consequences

Failure to comply with this policy may result in significant legal or regulatory sanctions, including fines, criminal liability, or reputational damage to Krevetka B.V. Employees may also face disciplinary action, including dismissal, if found to be involved in violations.

All employees must be vigilant, follow the policy at all times, and report any suspicious circumstances or potential breaches to the Compliance Officer without delay.

Roles and Responsibilities

Board of Directors

The Board holds ultimate responsibility for ensuring that the company's Sanctions Policy is effective. Their tasks include:

- Reviewing and endorsing the policy as needed
- Promoting a compliance-oriented culture
- Ensuring sufficient resources for sanctions and AML/CTF compliance

- Evaluating reports from the Compliance Officer
- Appointing a qualified Compliance Officer and giving them the necessary authority

Director(s)

Directors oversee the handling of escalated cases, especially those that involve legal complexity or conflicting jurisdictional rules.

Compliance Officer

This officer is responsible for:

- Conducting sanctions assessments related to clients and transactions
- Proposing policy updates and submitting them for approval
- Keeping relevant staff informed of changes in global sanctions regimes
- Ensuring the accuracy and completeness of client identification data

All Employees

Every employee at Krevetka B.V. must:

- Comply with all procedures outlined in this policy
- Be aware of the risks associated with sanctioned parties
- Immediately report suspected violations to the Compliance Officer
- Never advise clients on ways to avoid sanctions
- Complete training related to sanctions compliance within set deadlines

No employee is permitted to help or suggest to customers how to structure activities to evade sanctions. Such behaviour will result in strict disciplinary action.

Sanctions Screening

Krevetka B.V. applies continuous sanctions screening procedures to all customers, related parties, transactions, and third-party entities, both during onboarding and throughout the business relationship. The process is supported by an external sanctions

screening system that is updated in real time and cross-references global sanctions databases.

Match Categorization

When the system detects a possible match, it categorizes the outcome as follows:

- **True Positive:** A confirmed and complete match with one or more entries on a recognised sanctions list.
- **Potential Match:** Partial match with insufficient data to confirm (e.g., missing birthdate), or match linked to reputational concerns such as adverse media.
- **False Positive:** A match initially flagged but later disproven upon manual review.
- **Non-Criminal Match:** A match with a listed individual or entity not associated with criminal activity (e.g., media exposure).
- **Unknown:** The data provided is incomplete, preventing proper evaluation.

Cases classified as **True Positive** or **Potential Match** are escalated to the Compliance Officer for further analysis. If the customer is declined due to sanctions-related concerns, the reason for rejection is recorded with a corresponding classification, such as:

- Sanctions match
- Politically Exposed Person (PEP)
- Criminal record
- Adverse media findings

Sanctions Lists Covered

The screening process checks against a broad range of authoritative international sanctions lists, including but not limited to the following:

European Union (EU)

- European External Action Service (EEAS)
- Consolidated list under the Common Foreign and Security Policy (CFSP)

- Regulations targeting Russian entities and related restrictive measures

United Kingdom (UK)

- HM Treasury Consolidated Financial Sanctions List
- Bank of England (BOE) capital market restrictions
- Foreign, Commonwealth & Development Office (FCDO) sanctions list

United States (US)

- **Bureau of Industry and Security (BIS):**
 - Denied Persons List
 - Entity List
 - Military End User List
- **Office of Foreign Assets Control (OFAC):**
 - Specially Designated Nationals (SDN)
 - Programs related to Iran, North Korea, Russia, Syria, Cuba, Venezuela, etc.
 - Cyber sanctions, Global Magnitsky Act, CAATSA, and others
 - OFAC Consolidated Sanctions List (OFAC-CSL), which includes:
 - Foreign Sanctions Evaders (FSE)
 - Sectoral Sanctions Identifications (SSI)
 - CAPTA, NS-MBS, NS-CCMC, NS-ISA Lists

United Nations (UN)

- United Nations Consolidated Security Council Sanctions List, covering all UN-imposed measures

Ongoing Screening and Review

All customers are screened **before** their accounts are activated. Screening continues throughout the lifecycle of the customer relationship to ensure immediate detection of any newly issued designations or status changes.

Response Protocol for Confirmed Matches

If a match is confirmed, the Money Laundering Compliance Officer (MLCO) will apply the necessary response measures based on the relevant sanctions regime. These may include:

- Freezing of funds or accounts
- Declining or terminating the business relationship
- Applying financial restrictions, such as restrictions on capital instruments

Any actions taken are always assessed in light of legal obligations across jurisdictions, and, where conflicts of law arise, the issue is escalated appropriately to ensure legal compliance.

Sanctions Evasion

Krevetka B.V. acknowledges that attempts to circumvent sanctions regimes pose a significant compliance risk and may constitute an independent legal violation. Evasion of sanctions, whether direct or indirect, is prohibited under all major frameworks including those administered by the United Nations, the European Union, and the United States.

Examples of sanctions evasion include:

- An unsanctioned person purchasing digital assets, such as cryptocurrency, on behalf of a sanctioned company.
- Customers altering payment details following a transaction rejection to mask links to sanctioned entities. This practice is commonly known as wire stripping.
- A US-based customer using a virtual private network (VPN) to hide their location and perform transactions that would otherwise be restricted.
- Transfers routed through intermediaries or shell companies located in non-sanctioned jurisdictions, which ultimately benefit sanctioned entities.

Krevetka B.V. may detect evasion attempts during various phases of customer interaction. These include client onboarding, transaction monitoring, customer service communications, and ongoing due diligence. Any suspected evasion activity must be reported to the Compliance Officer without delay.

The Compliance Officer will conduct an investigation and determine whether further escalation is required. Indicators of sanctions evasion are also considered during high-risk client reviews conducted under the company's AML and CTF framework. If evidence of potential evasion is uncovered, it must be documented and included in compliance reports submitted to executive leadership and the Board of Directors.

Asset Freezing

Asset freezing, often referred to as blocking, is a critical enforcement tool under most sanctions regimes. If a customer is identified as having a direct or indirect interest in an asset and is subject to sanctions, Krevetka B.V. is legally obligated to freeze the associated funds.

This process does not transfer ownership of the assets, but it prevents the sanctioned party from accessing, controlling, or benefiting from them in any way unless explicitly authorised by the competent authority.

Assets subject to freezing include both fiat currency and digital assets such as cryptocurrency. Freezing is applied immediately upon confirmation of a sanctions match and remains in effect until lifted by the relevant authority.

Sanctions Compliance Training

To ensure awareness and proper implementation of sanctions controls, Krevetka B.V. integrates dedicated training on sanctions compliance into its overall compliance programme. This training is reviewed and updated regularly by the Compliance Officer to reflect changes in legislation, emerging typologies, and organizational risk exposure.

There are two tiers of training delivery:

- **Annual general training:** Provided to all staff to ensure a foundational understanding of sanctions regimes, compliance obligations, and internal policies.
- **Targeted role-based training:** Tailored to employees in functions that deal directly with customer onboarding, payment processing, transaction monitoring, or risk assessments.

New employees must complete sanctions training within 30 days of joining the company. Training content covers:

- Key sanctions regimes (UN, EU, UK, US)
- Common enforcement programs and their implications
- Sanctions evasion tactics and red flags
- Roles and responsibilities under internal policy
- Legal and operational consequences of non-compliance

All training records, including materials, assessments, and attendance logs, are retained in line with the company's legal obligations.

Outsourcing of Sanctions Compliance Activities

Where Krevetka B.V. outsources any portion of its sanctions screening or compliance activities, the company retains full responsibility for ensuring those services meet the applicable legal and policy requirements. Due diligence must be conducted on any service provider involved in sanctions compliance.

This includes:

- Evaluating the provider's internal controls and technical capabilities
- Assessing past performance and regulatory compliance history
- Establishing clear reporting obligations and oversight mechanisms

The Compliance Officer must maintain oversight and ensure all outsourced operations align with the standards set out in this policy.

Record-Keeping and Retention

All documentation related to sanctions compliance is retained in accordance with Krevetka B.V.'s internal policies and legal obligations. Records include:

- Sanctions screening outcomes
- Match investigations and resolution notes
- Training materials and completion records
- Internal escalation reports and regulatory notifications
- Correspondence with relevant authorities

These documents are securely stored, access-controlled, and retained for at least the minimum period (5 years) required by applicable laws and regulations.

12. Suspicious and Unusual Activity and Transaction Reporting

Krevetka B.V. recognises that the identification and reporting of suspicious or unusual activity are essential obligations within its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) programme. These responsibilities form a critical part of the company's efforts to detect and prevent criminal misuse of its gaming and betting services.

Timely and accurate reporting of suspicious activity not only ensures compliance with Curaçao's regulatory obligations but also protects the platform from legal, financial, and reputational harm. Furthermore, it plays a vital role in shielding customers from potential exploitation and upholding the integrity of Krevetka B.V.'s operational environment. Any failure to report such activity whether due to negligence or intentional omission may result in severe consequences, including regulatory sanctions or criminal liability.

Detection of Suspicious and Unusual Behaviour

Suspicious activity may emerge from transaction monitoring alerts or staff observations of atypical customer behavior. Indicators may include:

- Unstructured or unusually high-value deposits and withdrawals,
- Drastic changes in customer transaction patterns,
- Wagering behavior that appears inconsistent or indifferent to gaming outcomes,
- Signs of account usage inconsistent with the customer's risk profile,
- Attempts to conceal the true origin of funds or fund flows through third parties.

These red flags do not always indicate criminal conduct, but they must be reviewed and evaluated through the company's internal escalation procedures.

Internal Review and Escalation Protocol

Krevetka B.V. applies a two-tiered review model for assessing suspicious activities:

1. Preliminary Assessment

The Compliance Monitoring System or an employee may flag an activity as potentially suspicious. The initial review determines whether the behavior is explainable or represents a deviation that requires escalation.

2. Formal Evaluation by AML/CTF Officer

If suspicion persists, an internal Suspicious Activity Report (SAR) is prepared and forwarded to the company's designated AML/CTF Officer. This officer evaluates the available evidence and decides whether a formal report must be submitted to the Financial Intelligence Unit (FIU) of Curaçao.

All internal reports, regardless of the final outcome, must be documented and securely archived in compliance with the company's AML record-keeping requirements.

Filing Unusual Transaction Reports (UTRs)

As mandated under Article 1 of the National Ordinance on the Reporting of Unusual Transactions (NORUT), Krevetka B.V. must submit Unusual Transaction Reports (UTRs) to the FIU Curaçao via the goAML portal. This obligation has been in effect since 1 January 2021 and applies to all entities offering online gambling services under Curaçao's regulatory regime.

The AML/CTF Officer is responsible for:

- Determining whether an unusual activity meets the statutory criteria for external reporting;
- Filing the report through the goAML portal within the required time frame;
- Maintaining an internal log of the report, the rationale for filing, and any supporting evidence;
- Ensuring that staff involved in the process follow the internal reporting protocol outlined in the AML Policy.

If warranted by the nature or severity of the activity, the customer account may be temporarily frozen or permanently closed while the matter is under investigation.

Employee Reporting Duties

All employees of Krevetka B.V. are required to report any suspicion or reasonable belief that a customer may be involved in money laundering, terrorist financing, or related criminal conduct. This obligation applies even if the employee is uncertain about the exact nature of the suspicion. Reports must be submitted immediately to the AML/CTF Officer using the internal reporting channel.

Once a report is received, the AML/CTF Officer will assess the submission and determine:

- Whether additional information is needed;
- If the case meets the threshold for escalation to the FIU Curaçao;
- What actions should be taken to mitigate any ongoing risks.

12.1. Suspicious and Unusual Activity

Krevetka B.V. identifies suspicious activity by examining both transaction behavior and irregularities in customer profiles. The following indicators are treated as red flags and may prompt internal investigation:

- Recurrent use of anonymous payment instruments such as prepaid cards or vouchers.
- Discrepancies between customer geolocation and the origin of their funds.
- Large deposits followed by immediate withdrawals without corresponding gaming activity.
- Withdrawal requests made using third-party payment methods.
- Avoidance of identity verification procedures or reliance on proxy identities.
- Claimed financial status that does not align with the customer's spending activity.
- Frequent or unexplained changes in account ownership details.
- Reluctance or refusal to provide required due diligence documentation.

Each of these scenarios is documented in full, including associated dates, transaction types, amounts involved, and relevant customer data. The compliance and fraud prevention units conduct a structured assessment of the complete customer profile, including all gathered evidence, to determine whether further investigation or formal reporting is necessary.

12.2. Suspicious and Unusual Transactions

A transaction is deemed unusual when it significantly diverges from a customer's typical financial behavior or declared economic profile, particularly when lacking a clear and lawful explanation. Krevetka B.V. considers the following types of activity as potential indicators of concern:

- Unexpected or unjustified spikes in deposits or withdrawals.

- Transactions involving unrelated or previously unassociated third parties.
- Patterns of financial activity that contradict the customer's stated income or financial background.

The company operates an automated monitoring system that continuously analyzes transaction flows to identify such deviations. When anomalies are flagged, alerts are immediately forwarded to the Compliance Officer for assessment. Employees are trained to recognize behavioral and transactional red flags and to report concerns through the established internal escalation procedures.

Transaction Types Warranting Heightened Scrutiny

Certain transactions are categorized as requiring enhanced review due to their risk profile or regulatory relevance. These include:

- Transactions previously subject to reporting due to suspected links to money laundering or terrorist financing.
- Transactions involving individuals or entities listed under the Sanctions National Ordinance or other equivalent regulatory designations.
- Single or aggregated transactions within a 24-hour period that equal or exceed 5,000 Netherlands Antillean Guilders (NAF), regardless of whether they involve deposits, wagers, or withdrawals.

Whenever there is reasonable cause to suspect that a transaction may be associated with money laundering, terrorism financing, or proliferation financing, immediate escalation is required. Such cases must be reviewed by the Compliance team without delay to ensure appropriate action and timely reporting.

12.3. Timely Reporting

Once it is determined that a transaction qualifies as unusual or suspicious, Krevetka B.V. is required to promptly submit an Unusual Transaction Report (UTR) to the Financial Intelligence Unit (FIU) of Curaçao, in accordance with AML Regulation IV.1. This obligation applies even if the transaction was not executed or was merely attempted.

The Compliance Officer holds sole authority to submit the report without the need for additional approval. Timely filing is critical, as delays may constitute a breach of legal and regulatory obligations.

12.4. Confidentiality and Commitment to a Strong Reporting Culture

Strict confidentiality must be preserved regarding both Suspicious Activity Reports (SARs) and Unusual Transaction Reports (UTRs). Employees are strictly forbidden from

disclosing the existence, content, or status of such reports to the subject involved or to any unauthorized party.

Any such disclosure may be interpreted as tipping-off, which is a violation of Curaçao's legal framework and may jeopardize ongoing investigations. Only the Compliance Officer and a limited number of authorized individuals may access information related to suspicious transaction reports.

To reinforce this standard, Krevetka B.V. incorporates specific training on SAR confidentiality and reporting obligations into its AML and CTF employee training programs. Any breach of confidentiality procedures is treated as a serious compliance incident and may lead to disciplinary action, including termination of employment.

Commitment to a Strong Reporting Culture

Krevetka B.V. is fully committed to fostering a workplace culture rooted in vigilance, confidentiality, and accountability. This commitment enhances the effectiveness of the company's AML, CTF, and CPF framework, ensures continued alignment with regulatory expectations, and contributes to global efforts to combat financial crime in the online gaming and betting sector.

13. Compliance Officer

At Krevetka B.V., the Compliance Officer, also designated as the Money Laundering Reporting Officer (MLRO), holds a central and independent role in the governance and oversight of all Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) procedures. This position is critical to upholding the company's regulatory obligations and safeguarding the integrity of its internal compliance operations.

The Compliance Officer is the primary contact for all official communications with regulatory bodies in Curaçao, including the Financial Intelligence Unit (FIU). This individual also supervises the daily work of the AML compliance team and ensures the effective implementation of age verification measures, responsible gambling protections, and self-exclusion protocols in line with Curaçao's licensing requirements.

To ensure autonomy and impartiality, the Compliance Officer remains structurally and operationally independent from all commercial and operational departments. The officer is granted unrestricted access to internal platforms, customer profiles, transaction data, and any personnel necessary to fulfill compliance responsibilities. This role reports directly to the Board of Directors and is supported with appropriate authority and resources, as mandated under Regulation V.3 of the CGA AML Guidelines. This reporting structure guarantees that material compliance issues are escalated promptly and without interference.

In addition to internal compliance duties, the Compliance Officer is responsible for submitting all required Suspicious Activity Reports (SARs) to the FIU via the designated

goAML reporting portal. The officer also provides quarterly compliance updates to the Board of Directors, outlining risk trends, operational insights, and recommendations to strengthen the AML/CTF/CPF framework.

Core Responsibilities of the Compliance Officer

1. Policy Implementation and Supervision

- Oversees the application and enforcement of Krevetka B.V.'s AML/CTF/CPF policies.
- Ensures the internal framework remains aligned with evolving legal and regulatory expectations.
- Coordinates necessary revisions to compliance procedures and documentation.

2. AML Coordination and Liaison Duties

- Acts as the key liaison for internal and external AML-related matters.
- Communicates with regulators, law enforcement, and external auditors as required.

3. Monitoring and Reporting of Transactions

- Manages the company's transaction monitoring system to detect irregular or suspicious financial activity.
- Reviews and investigates internal reports of suspicious behavior and determines the necessity of filing reports with the FIU.
- Maintains accurate and secure documentation for all internal alerts and external submissions.

4. Training and Staff Development

- Designs and delivers AML training programs tailored to various roles within the organization.
- Keeps employees up to date on their obligations and responsibilities under the company's compliance framework.
- Updates training materials in response to regulatory changes, enforcement trends, or identified internal gaps.

5. Engagement with Regulatory Bodies

- Responds to supervisory requests, inspection outcomes, and official audits.
- Participates in compliance assessments and formal evaluations conducted by regulatory agencies.

6. Internal Audits and Risk Assessments

- Conducts periodic reviews of the AML/CTF program to identify deficiencies or emerging risks.
- Implements action plans to address control weaknesses and enhance compliance practices.

7. Documentation and Recordkeeping

- Maintains a complete audit trail of all compliance activities, including SAR filings, risk evaluations, training records, and correspondence with authorities.
- Ensures that all documents are stored securely and are accessible for regulatory inspections.

By fulfilling these duties, the Compliance Officer ensures that Krevetka B.V. operates a strong, effective, and compliant AML/CTF/CPF structure. The position plays an essential role in protecting the platform from financial crime and aligning the company with both national and international regulatory standards within the iGaming sector.

14. Senior Management

Senior management at Krevetka B.V. plays a pivotal role in ensuring the continued effectiveness of the company's AML, CTF, and CPF compliance framework. The Board of Directors mandates direct and active involvement of executive leadership in the oversight of financial crime risks and the strategic development of internal controls designed to mitigate such threats.

It is the responsibility of the appointed AML/CTF Officer to keep the Board informed of all material developments impacting the company's risk exposure or control environment. This includes submitting an annual compliance report that outlines the efficiency and adequacy of the AML/CTF/CPF controls, along with any deficiencies or emerging risks.

Annual and Quarterly Policy Review

Senior management holds ultimate accountability for ensuring that all applicable AML/CTF/CPF policies and internal procedures are reviewed at least once every calendar year. These reviews are informed by findings from monthly risk assessments, which help identify systemic weaknesses, evolving threats, and operational inefficiencies.

When necessary, the AML/CTF Officer may propose amendments to any policy or procedure. Such recommendations are evaluated and, if deemed appropriate, approved by the Board of Directors. This ensures that internal controls and compliance processes are dynamically adjusted in line with the company's risk appetite and regulatory obligations.

Oversight of Employee Training

The leadership team is responsible for overseeing the company's AML training program. It ensures that all staff, particularly those in high-risk functions such as finance, compliance, and customer service, receive regular, relevant training on how to detect, prevent, and report suspicious activities.

Senior management also ensures that AML/CTF/CPF training materials reflect the latest legal requirements, typologies, and internal process changes. Special emphasis is placed on building employee competence in detecting red flags, escalating suspicious activity, and applying due diligence measures effectively.

Internal Controls and Governance

Senior management is charged with maintaining a sound internal control environment throughout Krevetka B.V. This includes implementing proper segregation of duties, approval workflows, access controls, and transaction monitoring procedures to detect anomalies and ensure operational integrity.

Decisions, reviews, and procedural documentation are recorded in a structured and transparent manner. This ensures that the company remains audit-ready and that any activity linked to financial crime prevention is fully traceable and accountable.

Independent Audit and Assurance

To validate the effectiveness of the compliance framework, senior management commissions independent audits (as per Section V.5 of the Curaçao Gaming Authority's AML Guidelines) and internal assessments on a periodic basis. These evaluations are designed to test the design and operational effectiveness of AML/CTF/CPF policies, controls, and monitoring systems.

The results are submitted to the Board for review, and if weaknesses are identified, remedial actions are initiated with defined timelines for completion. This cyclical process

ensures continuous improvement and long-term resilience of Krevetka B.V.'s anti-financial crime measures.

15. Employee Training & Screening

Employees serve as the first line of defense in Krevetka B.V.'s AML/CTF/CPF compliance architecture. The company fosters a strong culture of integrity, ethics, and regulatory adherence by implementing a rigorous employee screening framework and delivering structured training programs tailored to the specific roles and responsibilities of its staff.

Employee Screening Programme

Krevetka B.V. implements a comprehensive Employee Screening Programme aligned with Regulation V.4 of the CGA AML Guidelines, applied both at the time of recruitment and on a continuous basis throughout employment, particularly for positions involving customer onboarding, financial operations, and compliance oversight.

Pre-Employment Vetting

Prior to employment, all candidates especially those applying for compliance-sensitive or client-facing roles are subject to the following background checks:

- **Verification of identity** and right to work using official government-issued documentation;
- **Criminal record checks** to identify past involvement in financial crime or misconduct;
- **Employment history verification** and reference checks to validate credentials and assess reliability;
- **Screening against international sanctions databases** and Politically Exposed Persons (PEP) lists using a reputable third-party screening provider.

Candidates who fail to meet the company's integrity standards or present undue compliance risk are disqualified from employment.

Ongoing Employee Monitoring

To ensure continued suitability for sensitive roles, Krevetka B.V. conducts ongoing employee screening, including:

- **Annual rescreening** of personnel in high-risk or control-related functions;

- **Event-triggered checks**, such as internal investigations, disciplinary matters, or job reassignments;
- **Monitoring of changes** in sanctions exposure, legal status, or PEP classification.

All screening records are securely maintained in line with data protection regulations and retained for no less than five (5) years.

AML Training & Awareness Programme

All employees whose roles intersect with AML/CTF/CPF responsibilities are required to undergo mandatory training during onboarding and attend annual refresher courses. Training content is customised by function and designed to ensure awareness of key obligations under the company's compliance programme.

The AML training covers the following core areas:

- Legal and regulatory requirements applicable to AML/CTF/CPF in Curaçao;
- Detection of suspicious behaviors and red flag indicators, such as:
 - Unusual betting patterns or transaction flows;
 - Use of third-party or anonymous payment methods;
 - Mismatches between claimed and actual financial behavior;
- Correct procedures for completing and submitting Suspicious Activity Reports (SARs);
- The importance of client confidentiality and data protection in handling compliance investigations.

Employees are clearly advised that non-compliance with internal AML/CTF obligations including failure to report suspicious activity may result in disciplinary sanctions, termination of employment, or criminal liability.

Internal Escalation & Reporting

All staff must escalate any suspicion of unusual or potentially unlawful behavior to the Compliance Officer without delay. This is facilitated through the internal reporting system, and staff are provided with clear guidance and templates for submitting SARs in a timely and accurate manner.

Confidentiality & Data Protection

Strict confidentiality is enforced across all compliance processes. Employees are prohibited from disclosing AML-related findings or investigations to any unauthorized parties. Such disclosures may constitute tipping-off, which is a serious offence under Curaçao law. Breaches of confidentiality are treated as major compliance violations and subject to disciplinary procedures.

By maintaining robust employee screening and continuous training, Krevetka B.V. ensures that its staff are well-equipped to uphold regulatory standards, detect and report financial crime risks, and support the company's overall compliance mission.

16. AML Compliance Audit

Krevetka B.V. acknowledges the critical role that internal audits play in upholding the effectiveness, reliability, and alignment of its Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) framework. These audits are treated not merely as formalities, but as integral components of the company's governance structure that reinforce transparency, accountability, and operational soundness. All audit outcomes are formally communicated to senior management and the Board of Directors to ensure prompt evaluation and remediation.

Frequency and Audit Initiation

The company undertakes AML compliance audits at regular intervals, with a minimum requirement of one audit per year. Additional audits are triggered in response to significant regulatory developments, internal restructuring, or incidents that may signal gaps in the compliance controls. These audits are conducted by internal or external professionals with no involvement in day-to-day compliance operations and who possess subject-matter expertise in financial crime prevention.

Scope of AML Audit

Each audit is structured to examine the integrity of the compliance program, with particular emphasis on the following areas:

- **Policy and Procedure Evaluation**

The audit assesses whether the company's AML, CTF, and CPF policies are current, compliant with applicable laws, and effectively implemented across departments.

- **Risk-Based Framework Review**

The audit reviews the adequacy of Business Risk Assessments (BRA) and Customer Risk Assessments (CRA), including the company's risk categorisation models and mitigation controls.

- **Transaction Monitoring and Suspicious Activity Reporting**
It evaluates the efficiency of the transaction monitoring infrastructure and the completeness and timeliness of Suspicious Activity Reports (SARs).
- **Customer Due Diligence (CDD) and Know Your Customer (KYC/KYB)**
File reviews are conducted to confirm that customer identification, verification, and beneficial ownership procedures are properly followed and recorded.
- **Sanctions Screening Mechanisms**
The audit verifies whether the screening tools used to detect matches against global sanctions lists are functioning effectively and updated regularly.
- **Employee Training and Screening Measures**
The audit checks whether the company complies with its training schedule, content relevance, and employee screening obligations under its AML framework.
- **IT and Data Controls**
System integrity checks are carried out to ensure that automated tools used in compliance processes operate accurately and securely, including risk-scoring engines and user access controls.

Reporting and Remediation

Upon conclusion, all audit findings are compiled into a formal report and submitted to both senior management and the Board, in compliance with Section V.7 of the Curaçao Gaming Authority's AML Guidelines. These reports detail any detected deficiencies, control failures, or policy gaps, along with practical recommendations for remediation and timelines for completion.

Where significant risks are identified, the Compliance Officer ensures that corrective measures are immediately escalated to senior leadership. Follow-up audits may be conducted to verify the implementation of corrective actions and ensure that risk exposures are reduced to acceptable levels.

Documentation and Regulatory Cooperation

Krevetka B.V. retains all records related to AML audit activities for no fewer than five years. These records are securely stored and made available to the Curaçao Gaming Control Board (GCB) upon request. This reflects the company's commitment to regulatory transparency and its ongoing effort to enhance its financial crime prevention systems.

17. Regulatory Access and Cooperation

Krevetka B.V. affirms its full commitment to engaging transparently and constructively with the Curaçao Gaming Control Board (GCB) and any other relevant regulatory, supervisory, or enforcement authorities. The company views cooperation with oversight bodies as a fundamental element of responsible governance and a cornerstone of its compliance infrastructure.

Access to Systems and Records

To support regulatory supervision, Krevetka B.V. grants unrestricted access to its systems, records, personnel, and procedures for the purpose of evaluating its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing controls. This access applies to both routine examinations and unscheduled inspections, whether conducted remotely or on-site.

The following categories of information are made available upon request:

- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) files
- Historical transaction records and payment activity
- Internal and external AML, CTF, and CPF risk assessments
- Policies, standard operating procedures, and compliance manuals
- Records of compliance-related communication and employee training materials
- Logs of Suspicious Activity Reports (SARs) and related internal investigations
- Audit trails and technical logs from compliance platforms and systems

The company ensures timely and complete disclosure of requested materials, whether for inspection, clarification, or technical review. This includes participation in system walkthroughs, live demonstrations, and the provision of supplementary data or documentation as needed.

Record Retention and Security

All regulatory records are retained for no less than five years or for a longer duration if required by law. These documents are stored in secure systems with safeguards that prevent unauthorized access, alteration, or loss. The company ensures that all sensitive information remains protected, traceable, and readily available for regulatory review.

Cooperation with Inspection Outcomes

Krevetka B.V. commits to acting on findings or recommendations issued by the GCB or any other supervisory body. This includes the timely implementation of remedial measures, submission of follow-up reports, and direct communication to confirm the resolution of any identified weaknesses or deficiencies.

Acknowledgement of Regulatory Examination Authority

Krevetka B.V. acknowledges the examination powers of the Curaçao Gaming Control Board (GCB) as prescribed in Section V.6 of the CGA AML Guidelines. The company affirms its obligation to fully cooperate with all supervisory assessments, whether scheduled or ad-hoc, and shall provide complete access to its AML/CTF/CPF systems, records, staff, and procedures. The company further acknowledges that the GCB is empowered to evaluate the adequacy and effectiveness of its compliance framework and may take appropriate regulatory or enforcement action where non-compliance or material deficiencies are identified.

Governance and Culture of Cooperation

This proactive stance toward regulatory cooperation is embedded in the company's governance model. Senior management fully supports transparent communication and collaboration with external authorities. By fostering a culture that prioritizes openness, accountability, and compliance, Krevetka B.V. reinforces its commitment to preventing financial crime and protecting the integrity of Curaçao's gaming and financial systems.

18. Internal Audit and Reporting

Krevetka B.V. maintains an independent internal audit function to assess and enhance the effectiveness, efficiency, and resilience of its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) compliance framework. These audits are fundamental to the company's governance structure and are conducted at least once per year, or more frequently when triggered by changes in the risk profile, new regulatory guidance, or significant operational developments.

Audits may be executed by Krevetka B.V.'s internal audit team or, where independence or complexity requires, by a qualified external third-party auditor. This approach ensures that the audit process is impartial, objective, and carried out with the necessary professional expertise.

Scope of Internal Audit Activities

The scope of each audit includes, but is not limited to, the following areas:

- Review of the company's AML, CTF, and CPF policies and procedures to confirm their adequacy, implementation, and regulatory alignment

- Evaluation of transaction monitoring systems and sanctions screening tools for functionality and risk coverage
- Verification of the accuracy, completeness, and timely submission of Suspicious Activity Reports (SARs)
- Examination of customer due diligence practices, including onboarding protocols and application of risk-based assessments
- Assessment of the AML training program, focusing on content relevance, training frequency, and employee engagement
- Inspection of internal governance structures, oversight functions, and record-keeping procedures
- Review of whether internal controls and system capabilities align with the company's risk profile and comply with applicable legal and regulatory requirements

Reporting and Follow-Up Actions

Upon completion of the audit, a formal report is prepared and presented to senior management and the Board of Directors, or to any delegated body with oversight responsibilities. The report includes:

- The methodology used during the audit
- Key findings and identified deficiencies
- Recommendations for corrective action
- Defined timelines for implementation

Senior management is responsible for ensuring that all audit findings are addressed in a timely manner. Corrective measures must be tracked and implemented fully, with documented follow-up and validation to confirm resolution.

Compliance with CGA AML Guidelines – Section V.5

In accordance with Section V.5 of the Curaçao Gaming Authority's AML Guidelines, Krevetka B.V. maintains an independent audit function to evaluate the design, implementation, and effectiveness of its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) framework.

This function is carried out by qualified personnel who are independent from daily compliance operations and possess the necessary expertise in financial crime risk management. The purpose of this audit is to test whether internal policies, procedures, and controls are appropriately designed and operating effectively in practice.

Findings of each audit are formally documented and reported directly to the Board of Directors, and appropriate remedial actions are implemented and tracked to resolution. The audit scope includes, but is not limited to:

- Risk-based approach methodology (BRA, CRA)
- Customer due diligence and EDD implementation
- Transaction monitoring and reporting systems
- Suspicious activity reporting processes
- Sanctions screening tools and procedures
- Staff training and awareness programs

Audit documentation is retained for a minimum of five (5) years and made available to the Curaçao Gaming Control Board upon request.

Record Management and Auditor Access

All documentation related to internal audits, including working papers, reports, supporting materials, and follow-up records, is retained securely for a period of at least five years or longer where required by law. These records are stored in a protected environment with safeguards to prevent tampering or unauthorized access.

To facilitate a comprehensive and effective audit process, the internal audit function is provided with full access to all relevant systems, personnel, documentation, and platforms. This unrestricted access ensures compliance with legal expectations and supports transparent oversight of Krevetka B.V.'s financial crime prevention framework.

19. Record-Keeping

Krevetka B.V. strictly adheres to all legal and regulatory obligations concerning the retention and management of records, ensuring that a complete and accessible audit trail is maintained for review by competent authorities when required. In line with applicable data protection regulations, all records are preserved in digital format for a minimum of five years, starting from the establishment of a business, commercial, or professional relationship with any employee, customer, or third party.

To support compliance with AML, CTF, and CPF requirements, the company has adopted formal procedures for storing and securing essential documentation. This includes, but is not limited to:

- Verified identity information and due diligence documentation for all clients
- Comprehensive records of transactions and related communications
- Internal Suspicious Activity Reports (SARs) and associated analysis
- Employee training records specific to AML, CTF, and CPF awareness
- Findings from internal and external audits related to the AML compliance framework

All documentation is maintained within secure and encrypted systems, safeguarded by strict access controls. Only authorized personnel may access these records, and all access events are logged and reviewed periodically. Routine audits of the recordkeeping system are conducted to confirm data completeness, accuracy, and security.

20. Appendices

Appendix 1: Customer Risk Calculator

Customer Risk Calculator

Client no.:

Name:

NEW total score:

0.00

NEW risk level:

Low

Onboarding specialist:

Last update date:

Category

Score

low

0-2

medium

3 to 4

high

5 to 6

unacceptable

At least 7

inaccessible

Risk Category	Question	Risk score	Risk level	Additional comments
Client	Customer's Age			
	Citizenship			
	Second Citizenship (if any)			
	Country of Birth			
Geography	Country of Residence			
	Does Customer have the status of PEP/RCA (Politically Exposed Person/Relative and Close Associate)?			
PROFILE				
Client	Purpose of account registration?			
Client				
Client				
SDF/SDW				
Client	Source of funds	average		
Client				
Client				
Client				
Client				
Client	Source of wealth	average		
INCOMING PAYMENTS				
Transactions	Average frequency of transactions			
Transactions	Expected total value of transactions per period (EAP)			
Transactions	Types of incoming payments	average		
Transactions				
Transactions				
Transactions				
Transactions				
Transactions				
OUTGOING PAYMENTS				
Transactions	Average frequency of transactions			
Transactions	Expected total value of transactions per period (EAP)			
Transactions	Types of outgoing payments	average		
Transactions				
Transactions				
Transactions				
Transactions				
Transactions				
Transactions	Reasons for outgoing payments	average		
Transactions				
Transactions				
Transactions				
BEHAVIOUR				
Products and Services	Please indicate services of interest	average		
Products and Services				
Products and Services				
Products and Services				
Products and Services				
CONFIRMATIONS				
Payment Channels	Channels	average		
Third-party involvement				
Access				
Onboarding				
Client	Adverse media level			
Other	Manual risk level adjustment based on the specialist judgement (if any):			Comment regarding manual risk adjustment: Summary of the applicant:

Appendix 2: Employee Onboarding & Screening Form

Employee Screening Program

This Employee Screening Program sets out the mandatory standards and procedures used to vet, evaluate, and continuously monitor all personnel employed or engaged by Krevetka B.V. It has been designed in line with the requirements of Regulation V.4 of the CGA AML Guidelines, which require effective screening both before employment begins and during the term of service.

A dedicated Employee Screening Checklist is used to support this Program. It must be completed in every case to ensure all procedures have been correctly followed.

Scope of Application

This Program applies to the following categories of individuals:

- All employees, whether permanent, temporary, or working on a contract basis
- Members of senior management, the Compliance Officer, and anyone involved in AML, CTF, or CPF functions
- Individuals engaged through third-party or outsourced arrangements who perform regulated or sensitive duties

No individual may be assigned to a sensitive or regulated function unless all applicable screening procedures have been completed.

Screening Requirements

Krevetka B.V. ensures that all personnel are reliable, qualified, and suited to their roles. The screening measures are aligned with the sensitivity of the role and are fully documented. The screening process consists of the following components:

- Pre-employment screening

- Fit-and-proper assessment (for designated positions)
- Ongoing employee monitoring
- Completion of the Employee Screening Checklist

1. Pre-employment Checks

Before onboarding any candidate, the Human Resources Department, working with the Compliance function, completes the following steps:

- **Criminal record check:** A check is conducted to identify any criminal convictions, particularly those related to financial misconduct, fraud, corruption, or other offenses linked to integrity risks
- **Verification of identity:** Candidates are required to submit valid, government-issued identification, which is verified for accuracy and authenticity
- **Education and certification verification:** Any relevant academic and professional credentials are independently confirmed
- **Employment history verification:** Previous roles, performance, and conduct are checked, taking into account applicable local regulations
- **Reference checks:** At least two professional references must be obtained. Any adverse findings are escalated to the Compliance team

Employment offers are not finalized until all pre-employment checks have been completed and the checklist has been reviewed and signed.

2. Fit-and-Proper Assessment

For senior or sensitive roles, a formal fit-and-proper assessment is carried out to determine the applicant's suitability. This assessment considers the following factors:

- **Integrity and reputation:** No history of disciplinary action, regulatory sanctions, or criminal convictions
- **Professional competence:** Appropriate knowledge, expertise, and experience, particularly in AML or regulatory roles
- **Financial reliability:** When allowed under local law, a review of financial background, including insolvency or bankruptcy
- **Independence and impartiality:** Review of any existing or potential conflicts of interest

The completed Fit-and-Proper Assessment Form is reviewed and signed off by the Compliance Department and must be retained with all screening documentation.

3. Ongoing Monitoring of Employees

- **Annual rescreening:** Individuals in compliance-related or high-risk roles are subject to periodic rescreening. This may involve criminal background checks, performance evaluations, and confirmation of continued eligibility
- **Event-triggered rescreening:** Re-screening is carried out if an employee transfers into a sensitive or regulated position, is subject to internal allegations, or when legal, regulatory, or role-specific changes occur
- **Conduct-based monitoring:** Any concerns about employee integrity, conduct, or suitability must be reported immediately by the relevant manager or Compliance team

All rescreening activities must be documented in the updated Employee Screening Checklist.

4. Documentation and Retention

Krevetka B.V. keeps complete records of all screening activities, which may include:

- Background check results
- Identification and qualification records
- Fit-and-proper assessments
- Completed checklists
- Internal communications, approvals, and any concerns raised
- Corrective or remedial actions taken

These records are stored securely and retained for at least five years, or longer if required by law. All records are made available to the competent authorities upon request and stored in accordance with data protection regulations.

Roles and Responsibilities

- **Human Resources:** Oversees the pre-employment screening process, ensures documentation is completed and stored, and refers any issues to the Compliance team
- **Compliance Officer:** Leads screening for roles involving AML responsibilities, approves sensitive appointments, and ensures Regulation V.4 is fully applied
- **Senior Management:** Provides necessary oversight and resources, reviews escalations from Compliance, and receives updates on screening practices and outcomes

Compliance and Enforcement

Any failure to comply with this Program, including missing documentation or omitted assessments, may result in disciplinary action, including dismissal.

Krevetka B.V. confirms that this Program is aligned with the CGA AML Guidelines under Regulation V.4 and is reviewed annually to maintain relevance and meet evolving legal and regulatory expectations.

New Employee Checklist

Employee Name & Position: _____

Start Date: _____

The following documents must be collected and verified prior to the employee's official start date. Please mark each item as received and verified.

1. Copy of national identity card or passport
2. Valid work permit (if applicable)
3. Proof of residence
4. Certificate of clear criminal record
5. Non-bankruptcy confirmation letter
6. Reference letter from previous employer
7. Professional licenses or certificates (if required for the role)
8. Curriculum Vitae (CV)
9. Good repute questionnaire
10. Diploma of higher education
11. Acknowledgement of AML and IOM policies
12. Signed Privacy Notice
13. Induction and initial training acknowledgement form
14. Signed Employment Agreement

Reviewed by HR: _____

Date: _____