

GROUP RISK POLICY & COMPLIANCE FRAMEWORK

Document Control

- **Document Version:** 2026.4
- **Target Audience:** Regulatory Licensing Authority (Curaçao Gaming Control Board)
- **Classification:** Highly Confidential / Regulatory Filing

1. PURPOSE AND SCOPE

This Group Risk Policy outlines the anti-money laundering (AML), counter-terrorist financing (CTF), and fraud mitigation frameworks deployed across our corporate ecosystem. This policy governs all operational brands under our group umbrella: **Betti**, **Casino Ways**, **Betmac**, and **Truststake**.

Our operational strategy enforces a centralized risk management framework. Every user across all brands is subject to identical risk-tiering, transaction evaluation, and escalation procedures to guarantee full compliance with licensing requirements.

2. MARKET FOCUS & RISK CATEGORIZATION FRAMEWORK

Regardless of the brand, every player is funneled through our centralized risk matrix and dynamically evaluated throughout the customer lifecycle. Accounts are designated into one of three distinct risk tiers:

None

[Onboarding / Lifecycle Trigger]

|

└─> LOW RISK ──> Standard CDD + Automated WL Engine

Monitoring

└─> MEDIUM RISK ──> Localized Velocity Spikes / Threshold

Recalibration ──> Manual Review & KYC Refresh

└─> HIGH RISK ──> Behavioral Shifts / Engine Score 9-10 /

Adverse Hits ──> Immediate Lock + EDD / SOW / SOF

- **LOW RISK:** Customers displaying standard, predictable recreational activity with zero system flags. Subject to standard Customer Due Diligence (CDD) and continuous automated monitoring via our integrated Whitelisting Risk Engine.
- **MEDIUM RISK:** Triggered automatically by localized transactional velocity spikes, technical alerts, or structural changes in the user profile. Requires mandatory periodic manual reviews and proactive lifecycle KYC updates.
- **HIGH RISK:** Triggered immediately by significant behavioral anomalies, severe transactional velocity issues, cross-brand fraud matches, or Adverse Media/PEP/Sanction alerts. Mandates immediate account restrictions, manual investigation by the Payments and Compliance teams, and mandatory Enhanced Due Diligence (EDD), including Source of Wealth (SOW) and Source of Funds (SOF) verification.

3. RETROSPECTIVE TRANSACTION REVIEW (RTR) METHODOLOGY

Our transaction monitoring strategy bifurcates into real-time technical checks and comprehensive historical reconciliations to capture sophisticated financial crime patterns.

Technical Integration: Whitelisting Risk Engine & PaymentIQ (PIQ)

Real-time transaction monitoring is anchored by our proprietary **Whitelisting Risk Engine** integrated directly into the **PaymentIQ (PIQ)** platform.

- **Dynamic Risk Scoring:** The engine analyzes incoming metadata, processing channels, and velocity vectors to assign a dynamic risk score to every single deposit and withdrawal attempt.
- **Continuous Monitoring:** The Payments Team reviews all generated risk scores on a daily operational loop.
- **Threshold Management:** Any transaction or aggregated series of transactions generating an outlier score (e.g., scores of 9 or 10) triggers an automated lock, diverting the account out of automated processing into immediate manual investigation.

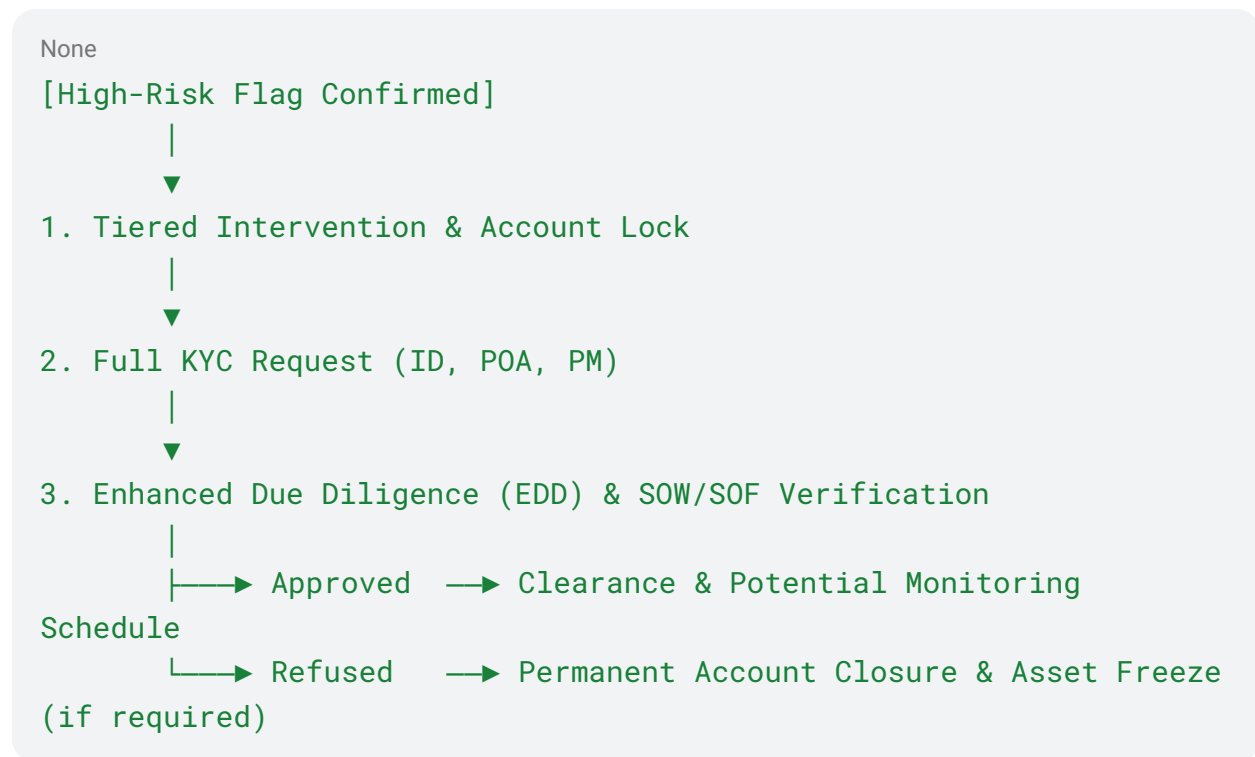
Frequency and Auditing Methodology

- **Daily Operational Reviews:** Continuous monitoring targeting high-risk flags, velocity spikes, and payment data discrepancies captured by the PIQ-integrated engine.

- Quarterly Retrospective Transaction Reviews (RTR):** Every three months, the Compliance and Analytics teams extract 100% of all transaction data processed during the period. This retrospective audit specifically analyzes historical datasets to detect macro-patterns that evade real-time transaction-level filters, specifically focusing on:
 - Velocity Patterns:* Gradual, systemic increases in deposit frequencies across extended periods.
 - Structuring Behaviors:* Deliberate fragmentation of transaction values to circumvent real-time automated velocity thresholds.
 - U-Turn Transactions:* Complex circular movement of funds across payment methods or associated accounts with minimal or no gaming activity.
 - Ad-Hoc Triggers:* Immediate macro-reviews initiated on specific player segments following systemic internal alerts or external threat intelligence.

Escalation and Remedial Actions

When an anomaly or high-risk flag is confirmed during a daily review or quarterly RTR, the Compliance team executes a strict, tiered escalation protocol:



- Account Restriction:** Immediate temporary suspension of deposit and withdrawal capabilities.
- Full KYC Request:** Mandatory collection and verification of Government Identification (ID), Proof of Address (POA) issued within the last 90 days, and Proof of Payment

Method (PM) utilized.

3. **Enhanced Due Diligence (EDD) / Source of Wealth (SOW) / Source of Funds (SOF):** If financial velocity is inconsistent with the established player profile, a formal SOW/SOF request is enforced. The player must provide certified documentation (e.g., payslips, tax returns, audited bank statements, legal documentation of payouts) demonstrating the legitimate origin of their capital.
4. **Permanent Account Closure:** If the user fails, refuses, or provides unauthentic documentation within the prescribed regulatory timeframe, the account is permanently terminated.

4. SCREENING TOOLS, ADVERSE MEDIA & LIFE-CYCLE TRANSITION

Current Status and Core Infrastructure Our company maintains a zero-tolerance posture toward sanctioned individuals and Politically Exposed Persons (PEPs).

Effective December 1st, 2025, our agreement with Sumsb was formally terminated. Accordingly the company has fully implemented and deployed a deep technical integration with SEON as our primary provider for real-time PEP, International Sanctions, and Adverse Media screening.

Data Retention & Audit Trail Preservation To maintain regulatory continuity following the Sumsb offboarding, the company initiated a formal data retrieval request to migrate 100% of historical screening logs, customer verification tokens, and compliance audit histories into our internal, highly secure, and encrypted storage. This guarantees that our historical compliance audit trail remains fully intact and available for regulatory inspection.

Post-Integration Verification Following the live deployment of SEON, our systems successfully executed a comprehensive batch screening of 100% of the customer accounts registered or modified during the transitional window. This retrospective scan ensured that no PEP, Sanctioned, or Adverse Media flagged individuals entered the ecosystem undetected during the vendor switch. Continuous real-time screening via SEON, alongside our internal PIQ-integrated Whitelisting Risk Engine, remains fully active to track behavioral, structural, and velocity anomalies.

5. REVENUE PROTECTION & BONUS ABUSE MITIGATION FRAMEWORK

To protect the financial integrity of our ecosystem against structured bonus abuse, predatory wagering strategies, and promotion-linked money laundering typologies, our company utilizes **Greco** as our primary risk mitigation engine.

Real-Time Bonus Abuse Monitoring & Action

- **Technical Integration:** The Greco platform is integrated directly with our player management systems to continuously monitor account behaviors during promotional campaigns, bonus clearings, and loyalty tier rewards.
- **Risk Mitigation Parameters:** Greco scans for specialized player abuse profiles, including:
 - *Coordinated Syndicates:* Multiple accounts placing correlated wagers to hedge risk and secure guaranteed promotional payouts across group brands.
 - *Irregular Wagering Patterns:* Dramatic adjustments in bet sizing or game selections immediately upon receiving or clearing promotional funds.
 - *Multi-Accounting for Promotions:* The creation of alternative identities to bypass household or device limits on introductory offers.
- **Automated and Tiered Intervention:** When Greco detects high-risk behavior, the system executes real-time countermeasures. These include the immediate revoking of current promotional rewards, stripping the profile of future bonus eligibility, or referring the profile to the compliance team for an account lock and an RTR investigation.

6. CRYPTOCURRENCY RISK POLICY & WALLET DISCLOSURE

Supported Virtual Assets

Our organization facilitates player transactions via designated virtual assets. To balance operational market demands with strict anti-money laundering (AML) controls, our platform restricts processing exclusively to the following cryptocurrency networks, as configured in our payment infrastructure:

- **Bitcoin (BTC)**
- **Litecoin (LTC)**
- **Ethereum (ETH)**
- **Bitcoin Cash (BCH)**

- **Ripple (XRP)**
- **Tether TRC-20** (USDT via TRON Network)
- **Tether ERC-20** (USDT via Ethereum Network)
- **Solana (SOL)**

Wallet and Exchange Arrangements

- **Closed-Loop Wallet Verification:** Players choosing to deposit or withdraw via virtual assets must use registered, auditable wallet addresses mapped directly to their verified customer profile.
- **Exchange Restrictions:** Currency exchanges within the player portfolio are strictly prohibited to prevent structural conversion manipulation. Payouts are processed natively in the corresponding virtual asset used for the initial deposit.

On/Off-Ramp Arrangements

- **Technical Integration:** Virtual asset processing is managed through a direct core integration via the **PaymentIQ (PIQ)** platform, routing through authorized crypto payment processing channels to handle network liquidity.

Blockchain Analytics & Screening Application

The internal **Whitelisting Risk Engine** applies real-time transaction-monitoring parameters to track blockchain data and intercept risk vectors:

- **Mixer Adjacency Controls:** The system tracks deposits for privacy protocols, obfuscation networks, or crypto mixers. Any detected adjacency triggers an immediate transaction rejection and account lock.
- **Peer-to-Peer Fraud Tracking:** Real-time behavioral models analyze on-chain data and transactional velocity to detect "chip-dumping" or asset-shifting tactics between colluding accounts.

7. CURAÇAO REGULATORY ALIGNMENT & LOK KYC MANDATES

Our compliance framework strictly adheres to the National Ordinance on Games of Chance (LOK), supervised directly by the Curaçao Gaming Control Board (GCB) acting as the ultimate independent regulatory authority.

Statutory Framework Alignment

This policy is fully aligned with the Financial Action Task Force (FATF) recommendations and the governing anti-money laundering and combatting the financing of terrorism (AML/CFT) laws of Curaçao, explicitly:

1. **NOIS:** National Ordinance on Identification when rendering Services (N.G. 2017, no. 92).
2. **NORUT:** National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99).
3. **Sanctions National Ordinance** (N.G. 2014, no. 55) and the **Kingdom Sanction Act** (N.G. 2016, no. 54).

Core GCB-Compliant Onboarding Standards

Pursuant to GCB B2C authorization requirements, we enforce a strict, risk-based approach to Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD):

- **Mandatory Verification Thresholds:** Anonymous or fictitious accounts are strictly prohibited. Identity verification requires authenticated government-issued identification, proof of residential address, and verified payment/wallet infrastructure documentation.
- **Statutory GCB KYC Thresholds:** In strict compliance with Curaçao AML/CFT regulations, our system triggers mandatory Customer Due Diligence (CDD) checks at the earliest practical time, and no later than when a player executes single or linked financial transactions totaling **NAf 4,000 (approximately EUR 2,000 to EUR 2,200)**. When this threshold is met, the system restricts the profile until identity and core credentials are fully verified.
- **Reporting of Unusual Transactions (goAML):** In accordance with the NORUT framework, any transaction or series of linked transactions equal to or exceeding **NAf 5,000 (approximately EUR 2,400)**, or any transaction deemed suspicious or uncharacteristic of the player's risk profile, is securely documented. The Compliance Officer files a formal report to the Financial Intelligence Unit (FIU) Curaçao via the integrated **goAML portal** within the statutory timeline.
- **Prohibition of Credit Facilities:** In compliance with Article 4 of the GCB general provisions, players must place wagers strictly against their own funded cash or virtual portfolios. Our system prohibits credit extension or the maintaining of negative balances in player portfolios under any circumstance.
- **Segregated Corporate & Player Accounts:** Player deposits and reward funds are kept in isolated financial infrastructure entirely distinct from the company's operational capital accounts. This protects customer balances and matches GCB financial stability mandates.

8. REVENUE AND COMPLIANCE AUDIT CASE STUDIES

Case Study A: Retrospective Fraud Identification & Multi-Accounting

- **User ID:** 40HMvLqscHm8v7yMeaux
- **Risk Designation:** High Risk
- **Trigger:** Daily manual Retrospective Transaction Review cross-referenced with an automated "High Risk" score generated by the Whitelisting Engine.
- **Investigation Protocols:** The Payments team performed a deep-dive forensic audit of the account history, payment tokens, and systemic session logs. The investigation exposed a highly coordinated pattern of cross-brand chargebacks executed across sister platforms, routed via a specific Payment Service Provider (PSP).
- **Remediation & Enforcement:** By cross-referencing hardware fingerprints and payment indicators across the group database, compliance confirmed sophisticated multi-accounting fraud. All associated accounts were immediately locked, services terminated, and the user profile permanently banned.

Case Study B: EDD, Source of Wealth Verification, and Responsible Gaming Escalation

- **User ID:** ygBWgPAvhxCgnxj7g3iH
- **Risk Designation:** Transitioned from Low/Medium to High Risk (Mitigated to Monitored Low)
- **Trigger:** Account registered on August 28, 2023, operating with standard low-to-mid-range deposit volumes for over two years with full baseline KYC clearance. On October 29, 2025, the daily PIQ engine flagged a massive velocity spike in weekly deposits completely outside historical trends.
- **Investigation Protocols:** An immediate full-account audit was triggered. Due to the extreme variance between historical recreational spend and the new velocity, a formal SOW/SOF request was mandated. The customer submitted comprehensive financial documentation. Compliance verified a legitimate, one-time lump-sum pension payout of €122,280.68 credited to the user's bank account on October 27, 2025.
- **Remediation & Enforcement:**
 - *AML Clearance:* The SOW/SOF documentation was officially authenticated, confirming a legitimate source of funds and mitigating money laundering risk.
 - *Responsible Gaming (RG) Intervention:* Recognizing the sudden liquidity influx, the compliance team routed the file to the RG department. A proactive customer outreach was conducted to ensure financial thresholds remained sustainable. While the account was left active, it was placed on a permanent **Weekly Monitoring Schedule** to guarantee continued player safety.

9. OPERATIONAL COMPLIANCE MATRIX (SAMPLE CUSTOMER COHORT)

The following matrix provides documented, visual, and operational audit steps executed for a standard cross-section of ten (10) actual customer accounts across various risk tiers, validating the real-world enforcement of this policy. Sensitive personal elements remain masked for GDPR compliance.

High-Risk Cohort (5 Clients)

Case 1: Real-Time Fraud Interception

- **User ID:** df456022-b361-46eb-94e6-375e273e4fb6
- **Registration Date:** February 3, 2026
- **Operational Scenario:** A newly registered user executed two rapid deposits totaling €90. The Whitelisting Risk Engine immediately flagged the activity with a maximum Risk Score of 10 based on systemic velocity parameters.
- **Compliance Action:** The Payments team immediately overrode automated processing, blocked the account, and placed the associated payment details into the global negative database.
- **Outcome & Regulatory Validation:** On February 5, 2026, the company received a formal Chargeback (CHB) notification for the deposits. The proactive engine block successfully mitigated further financial exposure.

Case 2: Shared Negative Database Cross-Brand Enforcement

- **User ID:** ca7be5ac-709d-44d3-9b6b-78d52af2c8d0
- **Registration Date:** January 24, 2026
- **Operational Scenario:** Upon account creation, the user attempted multiple rapid deposits. The Whitelisting Engine immediately blocked all processing attempts prior to capturing funds.
- **Compliance Action:** A manual Retrospective Review of the "Blocked Attempts" log was performed. Cross-referencing the underlying payment instrument tokens revealed a direct match with a previously terminated fraud account on a sister brand within the group.
- **EDD & Documentation Review:** The player was forced into EDD and instructed to provide high-level Identity and POA verification. The documents submitted were technically rejected (the player provided an unverifiable digital screenshot of the ID, and the POA failed to meet regulatory criteria as it was neither a utility bill nor a government-issued document).
- **Outcome:** Account remains fully blocked from funding, validating the efficacy of our shared multi-brand negative database.

Case 3: Zero-Tolerance Velocity & Cross-Brand Neutralization

- **User ID:** e745f2d3-6fb7-4d3b-985c-13b11cbc0863
- **Registration Date:** January 30, 2026

- **Operational Scenario:** A new registration occurred followed by immediate funding attempts. The Whitelisting Engine blocked the transactions instantly due to a metadata match on high-risk device parameters.
- **Compliance Action:** Manual investigation identified that the user's core physical details matched a high-risk fraud profile blacklisted on a sister brand for illicit chargeback histories.
- **Outcome:** In accordance with our group cross-brand risk policy, the new account was terminated, and all associated dormant accounts linked to this individual's personal data across all group platforms were systematically closed. Zero funds were permitted into the ecosystem.

Case 4: High-Risk Threshold Checkpoint Mitigation

- **User ID:** c1b2b32c-b692-4dc2-8e35-4107021071a0
- **Registration Date:** December 8, 2025
- **Operational Scenario:** The customer operated normally for two weeks until December 23, 2025, when a rapid series of deposits triggered a Risk Score of 9 within the PIQ engine.
- **Compliance Action:** The account was restricted under EDD. Compliance mandated the submission of a complete documentation suite: Proof of Identity (ID), Proof of Address (POA), Proof of Deposit Method, and Proof of Ownership (POO) of the underlying bank account to eliminate third-party funding risks.
- **Investigation & Outcome:** While documents were compiled, the team audited financial velocity, noting total deposits of €2,025 against €900 in withdrawals. The customer provided authentic, fully verified documentation. The High-Risk flag was successfully mitigated through transparency, and the account was cleared for standard operations.

Case 5: Real-Time Third-Party Payment Prevention

- **User ID:** 2fb03e52-9326-48d6-a67d-03de1d0cfe55
- **Operational Scenario:** During daily risk flag analysis, our team caught a successful deposit attempt where the payment instrument's cardholder name mismatched the first and last name registered on our gaming profile.
- **Compliance Action:** The transaction was flagged as a severe Third-Party Payment violation. Within 60 minutes, the Payments Team manually reviewed the file, permanently blacklisted the specific payment instrument on the user's profile to stop subsequent attempts, and suspended processing.
- **Outcome:** Attempted deposits were permanently rejected. The account was locked pending structural name reconciliation, and the user was notified of strict compliance mandates requiring all funding sources to bear their own verified name.

Medium-Risk Cohort (3 Clients) - Proactive Lifecycle Management

The following cases represent established, active players who reached the formal **Curaçao statutory KYC deposit threshold of NAf 4,000 (approx. EUR 2,000)**, automatically triggering our system tracking and lifecycle refresh protocols.

- **Case 6 User ID:** 8be011fd-1ff9-4a47-ae0f-f6a889a43b1c
- **Case 7 User ID:** f420e943-ce42-4dce-a29d-1b04cc52d406 (Alt Ref: ByelFo2vL76zi7WaKf5h)
- **Case 8 User ID:** 9c218f11-1fcb-412b-b9fa-7dc974c21c6a

Operational Scenario

Upon crossing the required statutory financial verification threshold, the system ran an updated verification check and triggered an internal alert showing that their previously verified identification documentation (ID or POA) had formally expired during their customer lifecycle.

Compliance Action

To maintain complete database integrity and comply with continuous monitoring regulations under the NOIS framework, the compliance system automatically executed the following steps:

1. **Immediate Deposit Block:** All three accounts were instantly restricted from executing any further deposit transactions.
2. **KYC Status Reset:** The verification status within our core CRM was manually reset to "Not Started." This hard system override ensures that no automated marketing or payment flows can bypass the documentation requirement.
3. **Refreshed Compliance Demand:** The users were issued automated and manual notifications stating that a full KYC refresh (current ID and utility/government POA issued within 90 days) is strictly required to restore account functionality.

Current Status

All three accounts remain strictly locked in a "Deposit Blocked" state pending the submission and successful validation of updated compliance documents.

Low-Risk Cohort (2 Clients) - Closed-Loop Withdrawal Verification

Our policy enforces a strict closed-loop policy, mandating full identity verification prior to the exit of any funds from the ecosystem, regardless of historical low-risk tiering.

Case 9: Automatic First Withdrawal Trigger

- **User ID:** 5d3aa83c-bae0-4a25-ac99-d267fcf0dd55
- **Operational Scenario:** A player with an entirely clean account history deposited an aggregate total of €725 with no velocity spikes or technical flags. The player subsequently generated winnings and requested a withdrawal of €1,150.

- **Compliance Action:** The system instantly placed the withdrawal request into a "Pending" status and triggered a mandatory KYC demand. The user is required to submit their standard suite: Identity (ID), Proof of Address (POA), and Proof of Ownership (POO) for both the depositing instrument and the receiving bank account.
- **Outcome:** The withdrawal remains held in our secure escrow environment until all documents are formally reviewed and approved by the Payments team, entirely eliminating account takeover or money laundering vulnerabilities.

Case 10: Total Traceability Threshold Override

- **User ID:** 444623d9-81c6-4301-8c98-c933300fc4d5
- **Operational Scenario:** A user deposited a nominal aggregate sum of €40. Despite this volume sitting vastly below baseline regulatory thresholds for standard due diligence, the player submitted a withdrawal request.
- **Compliance Action:** Our internal corporate risk policy dictates that **100% of first-time withdrawals trigger full KYC verification**, completely irrespective of the transaction value. The withdrawal was held, and a demand for standard ID, POA, and POO was applied.
- **Outcome:** The withdrawal is strictly withheld. This case establishes our operational commitment to Total Traceability—ensuring that no capital can move off-platform to an unverified individual, regardless of how minor the transactional footprint is.