

RISK, PAYMENTS, FRAUD (RPF) & AML COMPLIANCE OPERATIONAL MANUAL

SECTION 1: CORPORATE GOVERNANCE, LOCAL SUBSTANCE & REGULATORY MANDATES

1.1 Core Objective & Enforcement Context

The Risk, Payments, and Fraud (RPF) department protects the platform against financial crime, monitors and prevents fraudulent activities, mitigates anti-money laundering and counter-terrorist financing (AML/CFT) risks, and ensures stable transaction architectures across all operator brands

SECTION 2: SYSTEM TRANSACTION POLICIES & CLOSED-LOOP CONTROLS

2.1 Deposit (DP) Matrices, Limits & Market Variance

Transaction gateways are natively hardcoded to monitor and regulate payment parameters across various target markets. Payment visibility, specific currency ranges, and channel availability vary strictly by brand and market, with definitive parameters accessed via the profile Cashier layers or official Payment Policies.

- **Credit Cards & Alternative Digital Channels (Visa / MasterCard + Apple Pay/Google Pay):** Access is restricted exclusively to verified, Trusted users. System parameters enforce a minimum single deposit of **20 EUR** and a maximum cap of **2,000 EUR**.
- **Direct Bank Deposits:** Min DP: **20 EUR** / Max DP: **2,000 EUR**.
- **Crypto Asset Gateways:** Min DP: **20 EUR** / Max DP: **2,000 EUR**. Supported tokens: BTC, ETH, LTC, USDTE (ERC-20), and USDTT (TRC-20). Anonymous wallets, unknown mixers, or obfuscated token transfers are blocked; all digital asset channels must be completely transparent and auditable.
- **MiFinity Digital Wallet:** Market-restricted. Min DP: **20 EUR** / Max DP: **2,000 EUR**.

2.2 Withdrawal (WD) Matrices & Closed-Loop Directives

To systematically eliminate money laundering conduits and velocity exploits, the system applies a strict **Closed-Loop System**: payouts must route back to the identical payment method and matching account instrument from which the original deposit originated.

2.2.1 Closed-Loop Destination Rules

- **Credit Cards, AP/GP, & Direct Bank Deposits** Disbursed via Bank Transfer WD (the destination Bank Account details must directly connect to the verified deposit source instrument).
- **MiFinity Wallet Deposits** Disbursed exclusively back to the originating MiFinity Wallet account.
- **Crypto Wallet Deposits** Disbursed via Crypto Withdrawal matching the identical source token address on-chain.

2.2.2 Withdrawal Caps & Velocity Frameworks

- **Bank Transfer standard limits:** Min WD: **100 EUR** / Max WD: **2,000 EUR**.
- **MiFinity Disbursal:** Min WD: **100 EUR** / Max WD: **2,000 EUR**.
- **Crypto Transfers:** Min WD: **100 EUR** / Max WD: **2,000 EUR** (BTC, ETH, LTC, USDTE, USDTT).

SECTION 3: CORE ANTI-FRAUD PROCEDURES & RISK WORKFLOWS

3.1 Deposit Alert Handling & Third-Party Identification

Third-party funding attempts (depositing with a funding source where the owner's name does not match the registered player account name) are strictly prohibited. Transactions are monitored in real-time through the PaymentIQ (PIQ) engine and Back Office interfaces.

3.1.1 "PSP Account Used by Another User" Alert

This automatic rule triggers when a first-time depositor (FTD) or trusted profile uses a payment instrument already registered to a separate account, forcing an immediate transaction failure.

1. **System Query:** Extract the unique credit card/payment string, navigate to **User Accounts** in PIQ, and isolate all matching accounts.
2. **Instrument Audit:** Check card expiration dates to confirm whether they represent the exact same payment instrument.
3. **Cross-Account Correlation:** Open all associated profiles in BO. Assess hardware footprints via location, cross-brand activity flags, linked or duplicate accounts, third-party method history, and other suspicious behavior vectors.

3.1.2 Action Scenarios & Step-by-Step Remediation

- **Scenario 1: Failed Third-Party Attempt (Unlinked Source)**
 - *Action:* Block the card inside the **User Accounts** tab in PIQ. Select **Actions Block Account**, applying the reason **3rd party card- Not authorized**.
 - *Logging:* Append an explanatory note in BO: *"3rd party DP attempt with CCxxxx, keep an eye on, and if any successful deposits go through, request KYC and close down the account until verified. CC blocked."* Direct customer support to notify the user that third-party payment options are prohibited.
- **Scenario 2: Repeated Failed Third-Party Attempts**

- *Action:* Check for duplicate or associated profiles (linked/duplicates, shared CC holders). Apply a global instrument block inside PIQ. Evaluate total profile history to determine if full account termination is required based on the calculated risk.
- *Shared Instrument Exception:* If the payment method belongs to an existing registered player's profile, **Delete** the specific instrument association from the target account inside PIQ instead of blocking it, preserving the original owner's transactional ability.
- **Scenario 3: Successful First Time Depositor (FTD) Third-Party Event**
 - *Action:* Conduct an immediate risk assessment for linked or associated profiles using that method. If the underlying cardholder lacks a registered account, block the card via PIQ, issue an automated third-party warning alert, and log a comprehensive case file note. If the cardholder matches an alternate active registered account, execute the deletion protocol detailed in Scenario 2.
- **Scenario 4: Successful Trusted Player Third-Party Event**
 - *Action:* Perform a full risk assessment and review all linked profiles sharing the payment method. Block or delete (if a shared payment method) the card association inside PIQ. Based on historical account metrics, issue a final warning notice, place the account into immediate temporary suspension pending comprehensive verification, or permanently terminate the account depending on risk.
- **Scenario 5: Corporate or Business Cards**
 - *Action:* Intercept the corporate card variation and apply a temporary instrument lock via PIQ until KYC is completed. If confirmed via risk assessment that the player is the sole owner of the business, the card may be unblocked. Agents can request the entity VAT number directly from the player. If the user refuses to provide the VAT information, conduct open-source corporate check operations (via official corporate registries) to verify if the player is the sole authorized owner.
- **Scenario 6: Withdrawal Originating from Third-Party Funding**
 - *Action:* Freeze all pending payouts. Do not process pending funds or make independent processing choices. Block the payment instrument via PIQ and temporarily suspend the profile if needed. If the account is unverified, require full KYC. Escalate the case directly to management for review regarding asset confiscation, deposit refunds, or approved disbursal exceptions.
- **Scenario 7: Third-Party Deposit with Active Available Balance**
 - *Action:* Place the account into immediate suspension, lock the third-party instrument inside PIQ, and issue a full KYC directive. Once required documents are received and third-party involvement is confirmed, a warning can be issued. For joint banking configurations, the instrument remains blocked until formal verification confirms the card is legally in the customer's name, after which it may be unblocked.

3.2 Duplicate Account Lifecycle Management

Per LOK player protection guidelines and Term 2.8, users are legally restricted to one unique account profile per individual, physical name, household address, and IP footprint. Multiple accounts are strictly forbidden and trigger immediate closure protocols.

1. **Adjudication Principle:** Retain the oldest operational account footprint or the profile exhibiting the most significant historical turnover, deposit volume, and gameplay history. Close or restrict all duplicate accounts.
2. **Active Balances:** Once a duplicate profile is discovered, it must be locked immediately. Balances must be handled legally (confiscated & refunded), not gambled away.
3. **Pending Payouts & Complex Closures:** If a duplicate account holds an active pending withdrawal balance, close the account and escalate to management for review prior to executing any asset confiscation. If the original profile is flagged under an active Self-Exclusion (SE) order or permanently closed, freeze all access and escalate the file directly to management for a decision.

3.3 Chargeback (CBH) Recovery Procedures & Legal Defense

3.3 Chargeback Management & Risk Prevention Refunds

3.3.1 Definition, Exposure Risks & Discrepancies

Chargeback handling is a critical, high-priority task required to control the operator's chargeback rate and strictly mitigate financial losses. Credit card deposits inherently present significantly higher risk exposure compared to e-wallet solutions. Players may execute legitimate wagers, consume their balances, and subsequently file deceptive transaction disputes with their bank card issuer for the total deposited amount, directly exposing the brand to theft. Credit card networks are dynamically isolated at the bin/routing layer: Mastercard numbers always prefix with a **5** and Visa numbers prefix with a **4**.

The Structural Difference Between a Chargeback and a Refund

- **Chargeback (CHB):** An adversarial payment reversal initiated directly by the cardholder or their issuing bank. It strips the transaction funds from the merchant commercial account back to the issuer bank, carrying heavy additional administrative processor fees.
- **Refund:** A controlled capital repatriation initiated voluntarily by the merchant, relating strictly to a single card transaction. The returned amount can be whole or partial. Typical use cases include blocking restricted territories, patching technical provider glitches, or remediating internal tool bugs where a player accidentally bypassed self-imposed deposit limits. From a compliance perspective, returning the funds via a refund immediately clears liability.

3.3.2 Core Dispute Classifications

Disputes arrive within the dedicated network clearing terminal or via automated emails sent directly to the risk inbox at payments@betti1.com. Typically, these disputes surface within a window of **up to 9 months** post-transaction. Incoming items are divided into three legal categories:

1. **Malicious Intent (Fraud CHB):** Deceptive requests filed explicitly to regain lost funds after gameplay has occurred. No commercial exceptions are permitted; these profiles must be locked permanently.
2. **Bank CHB / Bank Risk:** Processing loops where the issuing institution automatically targets or flags the transaction under suspicious parameters or compliance flags, initiating disputes automatically.
3. **Friendly CHB / Legitimate Grounds:** Disputes originating from confusing merchant descriptors on statements (as descriptors do not feature the direct gaming site brand name), processing delivery lags, or family members utilizing hardware without permission. Commercial exceptions are reviewed under strict ad-hoc criteria.

3.3.3 Automated Intake Operations, Recording & Analysis

Dispute triage must be executed on a continuous daily basis, including weekends and public holidays.

Account Handling Workflow

Every disputed transaction must be tagged manually as **CHB** inside the the Back Office. Pin a permanent account note tracking the unique Transaction ID and total impacted volume (e.g., *“CHBs received for Txn id xxxxxxxx/20 EUR and txn id xxxxxxxx/30 EUR in the total amount of 50 EUR”*).

Recording Matrix

Immediately update the centralized spreadsheet registers to log operational actions and update the master tracking index:

Pattern Analysis

All items logged into the master spreadsheet must be cross-analyzed to capture organized fraud rings or velocity vectors. Analysis reviews shared registration metrics (IP addresses, physical cities, domain formats), financial markers (Bank BIN codes), gameplay vectors (initial game selection, highest turnover slots), or KYC background traits. Any pattern or suspicious activity detected should be escalated to management (Henke) to configure proactive security measures.

Dispute Rebuttals

Rebuttal letters and active representations are handled exclusively at the management level (Henke). By default, the current operational posture dictates a **no-dispute strategy**, which may be adjusted for high-value files or escalating transaction numbers under explicit executive authorization.

3.3.4 PSP Terminal Sourcing

Extract the transaction identification code from the PSP incoming notification email to track the player history within specific terminal interfaces:

- **DNS Gateway:** Transmits chargeback warnings via automated emails and updates the internal DNS Back Office. Locate updates within the top sub-menu of the **Orders** page, utilizing target filters to isolate active CHB flags from designated timeframes.
- **Payment Center (PC) Gateway:** Routes alerts directly via email. To audit inside the PC Back Office terminal, activate the **Filter** menu, access the **Type** parameters, and select **Chargeback**.

3.3.5 Risk Assessment & Profile Remediation Workflows

Locate the player identity using the transaction ID provided by the PSP. Cross-reference the identifier inside PaymentIQ (PIQ) and the BO to assess overall profile behavior:

- **Verify user account properties:** Determine the total credit card count used, matching names under PIQ User Accounts, historical revenue margins, VIP status tiers, and whether deposits were completed organically or manually pushed.
- **Isolate cross-gateway habits:** Verify if disputes target a single PSP gateway exclusively while alternate methods (e.g., IkaJo or GumballPay) remain undisputed. Log these multi-method scenarios inside the spreadsheet for advanced cross-gateway analysis.

Scenario 1: Confirmed Malicious Intent (Clear Fraud / Multi-Item CHB)

Triggered when there is undeniable proof of deliberate payment manipulation, characterized by multiple chargeback items (**3+ counts**), immediate account depletion patterns, or short-duration registration-to-dispute lifecycles.

- **Action:** Block the user profile permanently under the **"Fraud chargeback"** lock code. Add the transaction ledger note and update the master spreadsheet registers.
- **Cross-Brand Auditing:** Immediately query cross-brand databases to isolate linked sister profiles (e.g., matching Casinoways and Betti identities) and apply identical permanent blocks to both environments.
- **Fingerprint Restraints:** If the dispute count exceeds 3 chargebacks, flag and ban the account hardware and device identifiers within the Iovation console to block subsequent network registration attempts.

Scenario 2: High-Volume / Pinned High-Priority Monitoring

Triggered when an account registers an isolated, initial single chargeback count but exhibits positive historical revenue or high player lifetime values.

- **Action:** Apply a high-priority, pinned status warning note within the BO ledger.
- **Payment Blocks:** Navigate to PIQ $\rightarrow$ **Rules / Fraud Blocks / General Block**, and engage the **01 Specific user block** tool to instantly strip card deposition privileges across both operational brands.
- **Resolution Outreach:** Request Customer Support to initiate direct email outreach to collect a formal explanation. For these profiles, restrictions remain locked until a valid justification is produced, the funds are paid back, or management coordinates a targeted confiscation against active pending withdrawal balances on a case-by-case basis.

Approved Outreach Template

None

Subject: Urgent Account Verification Update - Transaction Inquiry

Dear [Customer's Name],

I hope this message finds you well.

We recently received a notification regarding a chargeback on your recent transaction made on [Date] at [Time] in the amount of [Amount] with us, and we are reaching out to better understand the situation.

At Betti, we value our customers and are committed to providing the best possible experience. To help us resolve this issue swiftly, could you kindly provide further details about the reason for the chargeback? We are eager to understand if there was any misunderstanding or concern that led to this action.

Please provide:

1. The reason for the chargeback
2. Any specific issues or concerns related to the product/service
3. Any additional feedback you may have

We are committed to resolving this matter promptly and amicably. Your feedback is very important to us, and we hope to clarify any issues you may have encountered.

Please note that during this investigation, access to your account may be limited or restricted until the matter is fully resolved. We apologize for any inconvenience this may cause and are committed to resolving this issue as quickly as possible.

We look forward to hearing from you and working together to resolve this. Thank you for your time and cooperation.

Best regards,
Risk & Compliance Department

Operational Communication Constraint: Support agents must remain neutral in their communication and inform the players that they need to contact their bank to cancel the dispute

Scenario 3: Single Transaction, Non-VIP Profiles

Triggered when a non-VIP player profile executes a minor initial deposit volume, consumes the balance, and immediately files a single chargeback item.

- **Action:** Terminate the profile permanently under the "**FRAUD CHB**" lock setting in the BO. Apply complete instrument blocks across PIQ. Do not transmit an informational alert or payment request email; the user is permanently excluded from re-opening and cannot pay back funds.

Scenario 4: VIP Tier Profiles & Managed Ad-Hoc Criteria

If an account exhibits an active VIP tag or meets specific ad-hoc indicators, the standard automated blocking sequence is bypassed. Route the profile directly to management (Henke) for ad-hoc validation if they meet any of the following parameters:

- Mapped under an active **VIP tag** with an established VIP Manager history.
- Cumulative deposit volume exceeds **€10,000**.
- The current chargeback ratio or dispute count is minor compared to their historical transactional turnover.
- The customer supplies clear cross-brand validation traits indicating legitimate, unflagged active profiles elsewhere.

Action: Do not transmit automated template warnings. Coordinate directly with the VIP Department to utilize their established, direct communication channels. The VIP manager will contact the player to gather details and coordinate a repayment process. Apply the standard PIQ user restrictions to block card deposits while the manual investigation is ongoing.

Scenario 5: Friendly & Bank CHB Remediation

Triggered by bank processing anomalies, merchant descriptor confusion, or verified accidental occurrences where no wider malicious intent or fraud ring patterns are discovered.

- **Action:** If a single descriptor misunderstanding or processing glitch is validated, log the context inside the account notes and update the master register sheets.
- **KYC Enforcement:** Issue an immediate demand for full KYC verification, including front/back credit card verification and bank statement proof of payment, before clearing the profile or lifting transaction boundaries.

Proactive Mitigation Controls

To minimize chargeback metrics and secure positive card processing states, agents must utilize the following proactive friction-reduction methods:

- *Processing Disclosures:* If withdrawal queues encounter heavy traffic volumes, support must provide the player with accurate, proactive updates and estimated completion dates to manage expectations and eliminate chargeback risk.

- **Transaction Notifications:** Ensure the automated system delivers clear email summaries immediately following a successful deposit, detailing the exact time, transaction date, and the specific statement descriptor used to prevent statement confusion.

3.3.6 Risk Prevention Refunds

Risk Prevention Refunds represent defensive financial adjustments executed on the processor or bank terminal to intercept high-risk algorithmic warnings before they mature into full chargebacks. These are triggered by payment processor algorithms or fraud flags on other external merchant networks.

- **Operational Rule:** If the player is verified as a legitimate customer or the alert represents a rare, single false-positive instance, bypass restrictions and monitor the account.
- **KYC Validation:** Enforce immediate, comprehensive KYC collection if the profile lacks documents.
- **Fraud Evaluation:** If the user profile exhibits clear fraudulent intent or accumulates **more than 7 counts** of automated risk prevention refund events, place the account into immediate restriction and review the file as an active threat. Note that players are unaware of processor-side risk calculations; actions must rely on case-by-case data reviews.

3.4 Missing Deposit Handling

When a missing deposit notification thread is received from the customer support partner (Betcare) via Slack, the RPF agent must execute the following tracking steps:

1. Locate the transaction details in the system backend. Agents require **4 critical tracking items**: *Player ID, Date of missing transaction(s), Transaction amount, and a Screenshot/PDF Bank Statement*.
2. Investigate directly inside the PSP Back Office using this data. If further details are needed, use the initial escalation thread.
3. Escalate the specific transaction ID and the respective Payment Service Provider (PSP) name back into the active support thread from Betcare on Slack.
4. Upon receiving a resolution or update from the PSP, locate the initial support thread by performing a global search (**Ctrl + F**) for the unique transaction ID on Slack to deliver the final status update.

SECTION 4: KNOW YOUR CUSTOMER (KYC) & CUSTOMER DUE DILIGENCE (CDD) PROTOCOLS

4.1 Risk-Based KYC Thresholds

None

[€2,000 Cumulative Threshold] —→ Triggers Mandatory CDD
(Primary POI + Valid POA)

[€10,000 Cumulative Threshold] —→ Triggers Advanced CDD (POI +
POA + Complete Proof of Payment)

[Suspicious Behavior/Crypto] —→ Immediately Triggers Enhanced
Due Diligence (EDD) + SOF/SOW Checks

- **Initial Regulatory Threshold:** Automatically triggered when a user's cumulative deposits or accumulated withdrawals reach **2,000 EUR** within a rolling 180-day window. Enforces mandatory Customer Due Diligence (CDD), requiring basic POI and POA.
- **Internal Threshold:** Automatically triggered when cumulative player transactions reach **10,000 EUR**, requiring POI, POA, and absolute verification of all payment instruments used.
- **Initial Payout Request:** Primary POI, POA, and active payment channel verifications must be cleared before an initial withdrawal is approved.
- **Enhanced Due Diligence (EDD) Triggers:** Required for elevated risk indicators: duplicate profiles, negative transaction patterns, or structural risk indicators. This process requires additional documentation such as payment methods proof of purchase, source of wealth, or face verification based on risk assessment. *Exception:* MiFinity wallet documents can be bypassed if a closed-loop history exists without risky behavior patterns.

4.2 Document Compliance & Verification Standards

Agents must evaluate document uploads against strict compliance criteria before updating system states:

- **Proof of Identity (POI):** Unexpired, government-issued Passport, Identity Card, Driver's License, or Residence Card. The document must display full name, DOB, issue/expiry dates, signature, and show all four physical corners.
- **Proof of Address (POA):** A high-quality photo or PDF utility bill, bank or credit card statement, or similar official document. The issue date must not exceed **3 months**
- **Credit Card Validation:** An official bank statement explicitly confirming ownership of the card
- **Proof of Payment (AP/GP & Payop):** Direct statement sent by the bank/financial institution showing bank/e-wallet name, physical address, account holder name, account address, account number, and the specific transaction. Apple Pay and Google Pay transactions require verification against authorized descriptors tracked via internal Slack logging resources. Payop wagers require a valid TransferOP payment statement.
- **Source of Funds / Wealth (SOF / SOW):** Valid bank statement coupled with an official corresponding employee payslip demonstrating regular legitimate income.
- **Third-Party Documentation:** Requires full, valid POI and POA (under 3 months old) belonging to the third-party individual.

- **Crypto Wallet Verification:** A screenshot or PDF of the crypto wallet profile or account settings showing the owner's full name or registered email address alongside the full wallet address. For non-custodial wallets where personal details are not displayed, a signed message from the wallet address or a video recording showing the logged-in wallet interface and the destination transaction hash is required.
- **E-Wallet Verification:** A high-quality screenshot or PDF of the e-wallet account details page. The document must clearly show the account holder's full name, email address, account ID/number, and the specific transaction details linking to the platform.
-

4.4 Technical KYC Management Pipeline

1. To identify these players, navigate to the **Users** section in BO, select **Alerts**, and enter the specified threshold amount (2k or 10k) in the Subject filter.
2. Add a **Documents Pending** tag on the account and request the files via the KYC dashboard. If requested directly under the KYC tab first, the system automatically appends the **Documents Pending** tag. The initial system status registers as **not started**.
3. Direct support agents to contact the user, instructing them to upload files via the secure AI verification tool within the profile cashier.
4. Upon thorough verification of POI and POA compliance, change the KYC status from **not started** to **Approved** or **Manually Approved** and move the toggle in the verified section to **YES**. This completely verifies the player within internal parameters and blocks subsequent automated verification engines from unnecessarily re-triggering the customer.

SECTION 5: RESPONSIBLE GAMING MANDATES & ACCOUNT ACTIONS

5.1 Account Closure Pipelines

- **General / Support Inquiries:** When a user requests closure via support, agents must request a valid reason. If handling live chat requests, support should offer tailored account deposit limits to prevent total closure. If handled via email, the account is locked immediately based on the user's instructions without offering limits. Players may also complete closures directly via the site under **Settings -> Your Limits -> Time Out**.
- **System Lock Configurations:** When terminating or restricting an account, agents must select the exact system lock type: **Customer Request** or **Problematic Gambling** if RG-related. All other input fields are left blank, and clear structural notes must be appended to the user profile (e.g., *"Account SE on CS req due to RG issues for 1 year"* or *"Closed permanently on CS req"*).

5.2 Responsible Gaming (RG) Limits & Adjustments

Players can manage deposit thresholds directly by navigating to the website **Settings -> Your Limits** interface.

- **Decreasing Limits:** Reductions in allowed deposit volumes take effect and go live immediately.
- **Increasing / Removing Limits:** Requests to remove or loosen limits trigger a mandatory **24-hour cool-down period**. The adjusted settings become active only after this cool-down window expires.

5.3 RG Re-opening Controls, Reconsideration Windows & PGSI Assessment

Standard accounts may be unlocked immediately upon request, except for profiles locked under fraud, abuse, or chargeback restrictions. Accounts restricted under a **Problematic Gambling** flag or general Responsible Gaming (RG) locks must undergo a strict compliance evaluation using the standardized **Problem Gambling Severity Index (PGSI)** framework.

5.3.1 Mandatory Screening & PGSI Testing

Support must issue an official compliance email containing the 9-item PGSI self-assessment questionnaire. The player is required to answer all 9 questions, scoring their behavior over the past 12 months using the standard format: *Never (0 points), Sometimes (1 point), Most of the time (2 points), or Almost always (3 points)*.

The evaluation covers the following regulatory assessment checkpoints:

1. Wagering more than the player can afford to lose.
2. Needing to gamble with larger amounts of money to get the same feeling of excitement.
3. Chasing losses (returning another day to win back money lost).
4. Borrowing money or selling assets to secure gambling funds.
5. Feeling that they might have a problem with gambling.
6. Gambling causing health problems, including stress or anxiety.
7. People criticizing their betting behavior or telling them they have a gambling problem.
8. Gambling causing financial problems for the player or their household.
9. Feeling guilty about the way they gamble or what happens when they gamble.

5.3.2 Declaration of Terms & Liability Disclosures

The evaluation email must explicitly state that the operator adheres to strict Curaçao Gaming Authority (CGA) player protection frameworks. It must explicitly inform the customer that **any subsequent or historical refund requests will be automatically rejected** upon account re-activation. If the portfolio holds an open cash balance, support must include a explicit disclosure explaining that manual platform payouts are unavailable, limiting their fund remediation options unless they choose to utilize the account interface directly.

5.3.3 Re-activation Logic & Risk Tiering

Following the player's submission of the PGSI test, support must tally the points to determine their risk profile:

- **Score of 0 (Non-Problem Gambler) or Score of 1–7 (Low-to-Moderate Risk):**
Support logs the score details in the account timeline and escalates the file to the Brand Management team for final review. If the brand approves re-activation, support applies a mandatory **24-hour cool-down/reconsideration lock** on the account. The agent must inform the player they have exactly 24 hours during which they can reverse their choice before the account goes live.
- **Score of 8 or Higher (Problem Gambler Profile):** The account fails the re-opening criteria. The profile **must remain permanently closed** under the **Problematic Gambling** system lock configuration. No manual overrides or subsequent applications are permitted.

SECTION 6: GDPR & PRIVACY DATA CONTROLS

6.1 Subject Access Request (SAR) Validation Protocols

To satisfy privacy data management standards, players requesting comprehensive ledger histories, transaction data, or personal profile sheets must execute a formal verification check strictly via their registered email.

6.1.1 Mandatory Validation Items

Agents must collect the following four validation items before processing an entry request:

1. The exact categories of personal data/information requested.
2. The precise historical timeframe referred to.
3. A complete, valid explanation and reason detailing the purpose of the data access request.
4. Both front and back sides of a valid, unexpired government POI (in JPG format) sent in the same email as proof of identity.

SECTION 7: BALANCE ADJUSTMENTS & CONFISCATION POLICIES

All asset adjustments, promotional capping actions, or balance confiscation updates must rely strictly on verified terms violations, backed by automated communication disclosures:

- **Third-Party Payment Breaches:** Executed under Section 4 (Deposits, Paragraph 2) and Section 13 rules. All generated winnings are removed, account portfolios are set to zero, and the primary deposit volume is refunded back to the originating funding instrument (the bank account connected to the credit card).

- **Duplicate Account Balance Confiscation:** Executed under Section 2 (Paragraph 7) and Section 13 rules. All assets, winnings, and conversions generated on duplicate profiles or under falsified registration names are confiscated, while the customer's primary original account remains active for use.
- **Bonus Cap Adjustments:** Executed under Section 7 of the Bonus Terms & Conditions. Winnings derived from shop free spins or no-deposit free spins are capped at a maximum payout of **100 EUR**. Excess funds are systematically removed when a withdrawal is requested.

SECTION 8: STEP-BY-STEP WITHDRAWAL PROCESSING CHECKLIST

The RPF team must execute these checklist steps in order for every pending withdrawal transaction inside BO:

1. **Slack Risk Sync Check:** Check internal escalation channels to ensure the player is not currently flagged or being investigated. If active investigations are open, leave the transaction pending.
2. **Device Analysis:** Query the Iovation interface to identify linked accounts, shared hardware configurations, or duplicates.
3. **Balance History Review:** Navigate to the player's account under the game activity/balances section and filter the user's balance history. Agents must filter strictly by these event types: **Bonus Converted**, **Deposit**, **Withdraw**, and **Rollback Deposit**. Check if winnings come from a bonus offer.
4. **Wagering & Turnover Audits:** Click the specific deposit that generated the current winnings and calculate user turnover. The deposit must be wagered through at least once) before any payout is approved.
5. **Bonus Abuse Assessment:** If wagers involve active promotional funds, review individual game rounds to ensure the user did not place bets exceeding the maximum allowed limit of **5 EUR**. Always check total bet logs.
6. **Session Security Check:** Review session histories to detect unexpected or unusual IP logging anomalies, proxy connections, or country shifts.
7. **Closed-Loop Verification:** Confirm that all payment methods used are verified and that the destination account matches the original funding source (closed-loop in place). For credit cards, verify that both the credit card and the bank account belong to the same bank and are under the customer's name.
8. **Final Action Routing:** If documentation requirements are not fulfilled within **24 hours** of withdrawal initiation, the agent must decline the transaction using the reason code **Documents not received**. If a third-party payment method was used, close the account right away and request all third-party documents. Otherwise, execute the **Approve** or **Decline** command directly within the BO transaction pipeline by clicking on the chain link for the pending withdrawal.

SECTION 9: GRECO ENGINE OPERATION & BONUS EXPLOITATION DETECTION

9.1 Purpose of Behavioral Tracking

The Greco platform acts as a real-time behavioral pattern monitoring and risk detection intelligence tool designed specifically for bonus abuse detection, exploitative gameplay, promotion misuse, and advantage play. It highlights unusual behavior and assists the RPF team in making informed decisions, moving investigations from reactive to proactive before significant financial losses occur.

Unlike fraud platforms (such as SEON, which focus on identity, payment routing, and multi-accounting), Greco monitors pure gameplay activity to identify patterns that comply technically with the rules but generate severe financial risk.

9.2 Structural Panels and Queues

- **Dashboard Interface:** Provides a high-level overview of overall statistics, triggered rules, active tags, and risk trends. Used to check general platform activity.
- **Players Section:** Serves as the primary active shift queue (daily work queue). Used to check flagged profiles, review active open tags, investigate review pending alerts, access player timelines, complete manual reviews, and analyze granular session histories.

9.3 Behavior Evaluation Infrastructure

9.3.1 Exploitable Slots Monitoring

Monitors players who target specific slot titles featuring mechanics that retain value between sessions (e.g., persistent bonus features, stored rounds, feature accumulation systems) to strategically accumulate value over time.

- **Rolling Risk Score (RRS):** A dynamic behavioral metric tracking how closely a player's style resembles documented advantage players. This score is continuously recalculated based on recent activity.
- **Stored Amount:** Potential value built up inside slot mechanics that has not yet been extracted.
- **Released Amount:** Realized winnings extracted from previously stored game features. *Operational Directive:* Released amounts require greater review priority since they represent actual financial value extracted from the business.
- **Observation Logs:** Details every daily metric shift, capturing lowest, highest, and final risk points alongside game providers (e.g., Play'n GO, Pragmatic Play, Evoplay), required spin durations, wagers, and specific risk score contributions. Expanding a date reveals specific round timestamps, stakes, and risk score adjustments. A steadily increasing score indicates more aggressive behavior than an isolated spike.

Exploitable Slots (ES) Tags Matrix

- **ES:** Exploitable Slots / **H:** High Risk (> 100\$) / **L:** Lower Threshold (< 100\$)
- **R:** Released Amount / **S:** Stored Amount
- *Configured Rules Examples:* **ES L 50 EUR R**, **ES L 100 EUR R**, **ES L 250 EUR R**, **ES H 50 EUR R**, **ES H 100 EUR R**, **ES H 250 EUR R** (Released Amount rules); **ES L 20 EUR S**, **ES L 40 EUR S**, **ES L 100 EUR S**, **ES H 20 EUR S**, **ES H 50 EUR S**, **ES H 125 EUR S** (Stored Amount rules). The higher the RRS and amounts, the higher the review priority.

9.3.2 Cash Stashing Analytics

Identifies players who deposit cash, receive promotional bonuses, and structure their play style to preserve their cash balance while forcing bonus balances to absorb the underlying wagering risk. Wagers are placed such that the cash balance is largely preserved (Cash Bet = Cash Win) while substantial bonus wagering activity takes place (indicated by high Bonus Turnover, a high Bonus Bet Count, and low cash bets).

Cash Stashing (CS) Tags Matrix

- **CS:** Cash Stashing / **SB:** Small Bet (\$0.01 - 2.99\$) / **BB:** Big Bet (3.00\$)
- **SW:** Small Win (\$0.01 - 2.99\$) / **BW:** Big Win (3.00\$)
- *Configured Markers:* **CS Warning** (Informational alert); **CS SB SW** (Small bet, small win); **CS SB BW** (Small bet, big win); **CS BB SW** (Big bet, small win); **CS BB BW** (Big bet, big win); **CS SP BB BW** (Sportsbook bet 10\$, win 12\$); **CS SP BB NO WIN** (Silent internal profile rule tracking sports bets 10\$ with no win).

9.4 Greco Shift Investigation Triage Sequence

1. **Timeline Analysis:** Open the player profile in Greco and check all triggered rules, timestamps, and active timeline event states (**Tag Added**, **Action Created**, **Action Applied**, **Tag Closed**). **Review Pending** signals an open alert requiring manual assessment before closing.
2. **Metrics Audit:** Evaluate key platform indicators (RRS, stored vs. released amounts, session numbers, and Bonus GGR). Expand the Session Logs to evaluate individual round IDs, game names, providers, cash bets, cash wins, bonus turnover, bonus GGR, and bonus bet counts. A high bonus bet count combined with very low cash bet values is a strong indicator of bonus abuse.
3. **Back Office Verification:** Cross-examine metrics inside the BO, analyzing total and average deposits, withdrawal histories, Net Gaming Revenue (NGR), net losses, historical bonus costs, and the overall Bonus-to-Deposit ratio. *Important Compliance Logic:* A player can trigger multiple behavior flags and remain highly profitable for the business; Greco findings must be evaluated alongside BO statistics before any restriction is considered.
4. **Profile Adjudication:** Evaluate whether the player only appears when bonuses are available, repeatedly triggers the same alerts, focuses heavily on specific games, or exhibits standard recreational behavior vs. strategic promotional optimization. Log the summary note on the account and execute the appropriate outcome:
 - *No Concerns:* Behavior is deemed periodic or recreational. Close review.

- *Monitor*: Actionable proof is insufficient but warrants observation. Add an account note and continue monitoring future behavior.
 - *Bonus Abuse Concern*: Systematic promotion exploitation is confirmed. Apply a formal Bonus Abuse Tag inside the account management settings to exclude the user from future promotional eligibility. Account closure is not normally justified solely on this activity.
 - *Escalation Required*: Multiple alerts, significant Released Amounts, high or increasing Rolling Risk Scores, or significant financial impact. Escalate for final decision; decisions must be based on facts, not assumptions.
5. **Resolution Execution**: To close an investigated alert, click the black circular check button corresponding to the target Manual Review line item. A pop-up will state *"This will trigger Manual Review for Player ID..."*; this is the correct system behavior and will close the active alert rather than creating a duplicate task.

SECTION 10: SEON SYSTEM OPERATIONS & REAL-TIME AML TRACKING

10.1 Screening Framework & Core Definitions

The SEON platform handles automated player identity validation, device analysis, and transaction compliance mapping, running automated checks against international Anti-Money Laundering (AML) databases.

- **Screening Action**: The precise point in time at which an identity profile is queried against global AML databases, generating active alerts.
- **Ongoing Monitoring Phase**: A continuous background integration process that scans the active player ledger whenever underlying global databases update or relevant personal data changes. The monitoring toggle functions as an active infrastructure indicator; agents do not manually engage or disengage monitoring profiles.
- **Shift Queue Rule**: Agents must access the left-hand panel **AML Tab HIT Section** every 2 hours. Investigations must always process chronologically, starting from the **oldest alerts first** to ensure no cases remain unattended.

10.2 AML Hit Categorization & Mandatory Protocols

SEON classifies database alerts into four risk categories. Agents must filter and prioritize these hits systematically, resolving the highest regulatory and legal risks first.

None

[TIER 1: SANCTIONS] —→ National Security & Terror Risks —→
Confirmed: Immediate Account Block & Escalate

[TIER 2: PEP CORES] —→ Public Figures & Associates —→
Confirmed: Profile Restriction + Launch EDD

[TIER 3: CRIME LISTS] → Financial/Adverse Media Records →
Confirmed: Risk-Weighted Context Check
[TIER 4: WATCHLISTS] → Insolvency & Civil Registries →
Confirmed: Identifier/DOB False Positive Audit

10.2.1 Sanctions Lists (Priority Tier 1)

- **Risk Parameters:** Individuals or corporate entities legally restricted or prohibited due to national security threats, war, international policy, embargoed jurisdictions, weapons trafficking, or terrorist activities/financing.
- **System Action:** Represents the highest legal and regulatory liability. If a sanction hit cannot be instantly categorized as a false match, the agent must immediately **restrict and block the player account** without delay, freeze all transaction capabilities, and execute a Tier 3 escalation.

10.2.2 Politically Exposed Persons (PEP) (Priority Tier 2)

- **Risk Parameters:** Individuals holding prominent public or state roles (e.g., presidents, prime ministers, ministers, MPs, mayors, senior military/police officials, high-court judges, state-owned enterprise heads, diplomats) and their close family members (spouses) or direct business associates. They represent enhanced risks for bribery, corruption, and the abuse of public power.
- **System Action:** Confirmed or highly probable matches require immediate **account restrictions** and must be routed directly into Enhanced Due Diligence (EDD) workflows.

10.2.3 Crime Lists (Priority Tier 3)

- **Risk Parameters:** Global records and adverse media profiles mapping to criminal activity, specifically financial crimes (fraud, tax evasion, money laundering, corruption, bribery, identity theft, forgery) or severe offenses (cybercrime, human trafficking, organized crime).
- **System Action:** Conduct a contextual assessment prioritizing financial crimes relevant to gambling operations, verifying the recency of the events and validating matching identifiers. Financial crimes always raise concern and serve as the starting point of the assessment.

10.2.4 Watchlists (Priority Tier 4)

- **Risk Parameters:** Informational public records, including civil bankruptcies, insolvency records, liquidation proceedings, director disqualifications, public registers, or charity, volunteering, and non-profit organization rosters.
- **System Action:** Review context, timelines, and identifiers (especially DOB) to separate high-frequency false positives from actual AML exposure.

10.3 Verification Triage Pipeline

When validating an active alert from the filtered screening view, select the player to open the Player Summary panel. Click **View Hits** on the left-side AML section to expand all external AML database match profiles, which must be evaluated individually.

Step 1: Core Identifier Validation

Every AML review must begin with a comparison of basic identifiers: *Full legal name and spelling, Date of Birth (DOB), and Country or nationality*. **The DOB is the single most critical identifier.** In many cases, a clear discrepancy between the player's registered DOB and the database record is sufficient to conclude that the alert is a false match.

Step 2: Chronological Timeline Validation

Analyze chronological records before starting open-source investigations to determine if the timeline makes sense.

- *Example:* If an AML profile indicates that an individual held an active Member of Parliament seat in the year 2010, but the player's registered DOB is 2006, this implies they held senior political office at age four. This is a logical impossibility; resolve the alert as a **False Match**.

Step 3: Open-Source Intelligence (OSINT) Checks

If identifier databases lack clear links or comprehensive details, perform targeted open-source verification. Use Google searches first, followed by social media and professional directories (such as LinkedIn, Facebook, and Instagram) to verify age, employment timelines, educational history, public roles, locations, or political exposures.

Step 4: Cross-Brand Database Synchronization

Audit cross-brand accounts across operator environments (e.g., Betti, Casinoways) to check for matching KYC data packages. Comparing uploaded document photographs, official birth dates, and nationalities across brands often resolves uncertainty in cases with unconfirmed results.

Step 5: Final Resolution Input & Note Logging

- **False Match Entry:** This option can only be selected when there is **100% confidence** that the database profile does not belong to the player. If any uncertainty remains, the alert must remain open or be routed through the escalation matrix. Repetitive common names are expected on AML lists and do not indicate a configuration error; eliminate false matches early using these standard identifier checks.
- **Mandatory Ledger Documentation:** Every single AML check decision requires complete documentation in the profile ledger to protect both the agent and the company. Notes must state exactly what metrics were verified, why the conclusion was reached, which identifiers were decisive, and should include live URLs to open-source profiles that prove the mismatch.

SECTION 11: INCIDENT RESOLUTION & OPERATIONAL ESCALATION TIERS

11.1 Gameplay Auditing & High-Win Verification

If an agent or support representative requests an investigation into a customer's game round due to a significant win, it will only be processed if the single game round win is **5,000 EUR or greater**. Game providers do not permit win verification for lower amounts, and general session audits are evaluated strictly on a case-by-case basis.

11.1.1 Step-by-Step Technical Audit

1. Navigate to the player's profile and open the **Game Activity** section. Select **Game Sessions** or **Game Rounds** and apply the relevant date filters to narrow down the gameplay details.
2. Review the transaction chain link and copy the unique **Game Transaction ID** (the win transaction ID).
3. Alternatively, navigate to the **Balances/View all Balance changes** section. Click on "View all Balance changes", use the filters to tick the **Win** box under reason, and set a minimum amount of 5,000. Filter dates starting from the last deposit associated with the winnings up to the last withdrawal request to examine balance movements.

11.1.2 High-Win Escalation Sequence

- **Target Workspace:** Alert the Casino Operations team immediately via the dedicated Slack channel ([crm-rpf](#)).
- **Required Metadata Payload:** Every message must include the Customer ID (CID), the Game Transaction ID, and the specific Game Provider.
- **System Logging Requirement:** Log a clear note on the player's account stating that the gameplay has been escalated for a Game Provider (GP) check, and update the profile notes once the legitimacy of the win is officially confirmed by the provider.

11.2 Comprehensive Structural Escalation Matrix

TIER 1: FRONT-LINE OPERATIONS (Customer Support & Level 1 RPF Agents)

Operational Focus: General triage, daily monitoring, standard request processing, and basic alert management.

- **Front-Line Inbound Requests:** Intercepts incoming tickets, manages standard customer requests, processes basic KYC document requests, and handles standard self-directed account limit reductions.
- **Daily Risk Triage:** Conducts daily transaction monitoring, basic duplicate checks, and routine fraud triaging.
- **Withdrawal Approvals:** Directly processes and approves standard, non-suspicious withdrawals within the standard terms limit of up to €15,000 per month.
- **SEON AML Screening:** Filters and reviews the SEON AML HIT queue every 2 hours, processing chronologically from the oldest alerts first.
- **Greco Engine Screening:** Audits and reviews Greco Manual Review queues at the start of every shift.



ESCALATION TRIGGER 1: Target Alerts & Specific System Metrics

Move to Tier 2 if the account triggers a specialized tool alert, missing funds request, or high-value win flag.



TIER 2: SPECIALIST CHANNEL / PARTNER INTEGRATION (RPF Specialists)

Operational Focus: Deep-dive investigations, partner network communications, and tool-specific risk management.

- Missing Deposits Workflow: Collects the 4 mandatory metadata payload items (Player ID, Date, Amount, Statement), logs the investigation in the PSP Back Office, and tracks resolution threads through the dedicated Slack integration.
- Technical Win Audits: Audits single game round wins equal to or exceeding €5,000 and escalates the data directly to the Casino Operations team via the [crm-rpf](#) Slack channel for Game Provider verification.
- PEP Alerts: Manages confirmed or high-probability Politically Exposed Person (PEP) database alerts. Applies immediate account restrictions and initiates the complete Enhanced Due Diligence (EDD) profiling sequence.



ESCALATION TRIGGER 2: Critical Risks, Material Deviations & Confirmed Hits

Move to Tier 3 if the case represents an absolute legal infraction, severe contractual breach, or high financial exposure.



TIER 3: SENIOR MANAGEMENT ESCALATION (MLRO / Executive Management)

Operational Focus: Final legal decisions, asset confiscations, out-of-scope approvals, and direct regulatory exposure handling.

- Out-of-Scope Disbursals: Final review and approval of exceptional withdrawal volumes that exceed the standard €15,000 monthly contractual limit.
- Third-Party Funding Infractions: Final adjudication and execution of balance confiscations or refunds for winnings generated from confirmed third-party deposits.
- Duplicate Profile Balances: Final review of duplicate account closures involving open cash balances or active pending withdrawals.
- Self-Exclusion Breaches: Direct handling of duplicate profiles created by players with an active Self-Exclusion (SE) status on their original account.
- Advanced Greco Exploits: Final resolution of high-priority Greco behavior profiles displaying a Rolling Risk Score (RRS) $\geq$ 200 alongside high Released Amounts.

- Confirmed Sanctions List Matches: Handles absolute matches against international Sanctions databases. Restricts the account immediately, freezes all asset movements, and manages the regulatory response.
- Enforcement Directives: All final Tier 3 decisions must rely strictly on documented, verifiable facts—never on operational assumptions.