

Cash Handling and Agency Intermediaries Policy

Document Control

Field	Detail
Document Title	Cash Handling and Agency Intermediaries Policy
Operator	Slotbox N.V.
Version	V2
Effective Date	July 2026
Review Date	June 2027
Classification	Confidential — Regulatory Submission
Policy Owner	Compliance Officer / MLRO
Approved By	Board of Directors — Slotbox N.V.
Regulatory Jurisdiction	Curaçao (CGA/LOK)

1. Introduction and Purpose

This Policy is in line with the Company's ongoing AML/CFT compliance obligations under the National Ordinance on the Identification of Clients when Rendering Financial Services (NOIS); the National Ordinance on Reporting of Unusual Transactions (NORUT); the Landsverordening op de kansspelen (LOK, December 2024); and the CGA Regulations for Combating Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction.

This Policy establishes the Company's framework for:

- Ensuring that physical cash plays no role in any payment channel;
- Defining permitted digital payment methods and the controls governing their use;
- Governing relationships with agency intermediaries and PSPs;
- Applying AML/CFT controls specific to the Company's payment channels; and
- Assigning governance and accountability for payment channel compliance.

This Policy supplements and cross-references the Company's AML/CFT Policy, Cryptocurrency Risk Policy, and Customer Acceptance Policy.

2. Scope

This Policy applies to:

- All deposit and withdrawal transactions processed by the Company or on behalf of players;
- Payment Service Providers;
- E-wallet operators, voucher issuers, open banking providers;
- Cryptocurrency VASPs engaged by the Company;
- All directors, officers, employees, contractors, and third parties acting as agents or intermediaries in the processing of player funds; and
- All geographies in which the Company accepts player registrations and deposits.

3. Cash

3.1 Position

The Company maintains that physical cash is not accepted in connection with player accounts or gaming activity.

The following are explicitly prohibited:

- Acceptance of physical currency (banknotes or coins) from players as a deposit;
- Disbursement of physical currency to players as a withdrawal;
- Acceptance of postal orders, money orders, or bearer instruments as a substitute for cash; and
- Use of cash as collateral, credit security, or any instrument that would result in a player gaming on credit.

3.2 Cash-Equivalent Instruments

Certain prepaid and voucher-based instruments may be accepted as deposit methods where they are issued by a regulated third-party PSP, fully traceable to an identified payer, and subject to the Company's due diligence requirements. For such instruments to be treated as permitted payment methods rather than cash equivalents, all of the following conditions must be met:

- The instrument is purchased electronically or via a regulated retail channel with a documented transaction record;
- The voucher code or PIN is applied directly to the Slotbox cashier by the player through the digital platform — not via a staff member or intermediary; and
- The issuing PSP is subject to the intermediary due diligence requirements set out in Section 5.3.

Where any of the above conditions cannot be met, the instrument is treated as a cash equivalent and is subject to the same restrictions.

Player-attributed payment wallet instruments that satisfy all three of the following criteria are treated as permitted e-wallet equivalents under Section 4.1 and are not subject to the cash-equivalent conditions above: (a) the instrument is issued exclusively in the player's verified name;

(b) it operates on fully electronic payment rails under the control of an entity subject to equivalent AML/CFT obligations; and (c) it is subject to the same KYC requirements as the Company's registered e-wallet providers.

3.3 Regulatory Requirements

The Curaçao AML/CFT framework explicitly prohibits online casinos from accepting cash as a payment method. However, the combined effect of the NOIS identification obligation, the NORUT unusual transaction reporting requirements, and the CGA AML Regulations renders cash structurally incompatible with lawful online gaming operations. The restriction stated in this Policy is consistent with compliance with mandatory Curaçao law.

NOIS — Identification at point of service. NOIS requires an operator to identify every client before or at the point of rendering a financial service. For an online casino, this means full KYC must be completed before a player can deposit or play. Physical cash cannot satisfy this requirement: it is anonymous at the point of receipt, carries no transaction record traceable to a named account holder, and cannot be reconciled to a verified identity in the way that a card payment, bank transfer, or e-wallet transaction can. Any deposit that is made in cash would leave the operator unable to produce, upon CGA or FIU request, the identification record required by NOIS for that transaction.

NORUT — Cash as an unusual transaction indicator. The Regeling indicatoren ongebruikelijke transacties (PB 2015, no. 73, as amended by PB 2024, no. 60) lists cash transactions among the objective indicators for unusual transactions that must be reported to FIU Curaçao via goAML. Any cash transaction at or above NAf. 5,000 (approx. EUR 2,500) triggers a mandatory Unusual Transaction Report (UTR) within 48 hours regardless of whether the operator suspects money laundering. For an online operator that accepts cash deposits, every material cash transaction would simultaneously be a reportable unusual transaction and an unidentified transaction under NOIS — a position that is operationally unworkable and inconsistent with the CGA's expectations of a licensed operator.

CGA AML Regulations — CDD and transaction monitoring. The CGA Regulations for the Combating of Money Laundering and Financing of Terrorism (January 2025, mandatory from 10 April 2025) require all licensees to apply customer due diligence to every payment, maintain full transaction records, and implement transaction monitoring systems capable of identifying suspicious patterns. Cash frustrates each of these requirements: it cannot carry an embedded identity, it leaves no auditable digital trail at the point of receipt, and its fungibility makes source-of-funds tracing materially more difficult than any regulated digital payment method.

FATF alignment. The cash restriction reflects FATF Recommendation 10 (Customer Due Diligence), which requires financial institutions and designated non-financial businesses and professions — including online gaming operators — to apply CDD measures when establishing a business relationship or carrying out occasional transactions above applicable thresholds. FATF guidance specifically identifies cash-intensive businesses and anonymous payment methods as elevated ML/TF risk factors. The CGA, as the AML/CFT supervisor for the online gaming sector (appointed January 2019), applies FATF standards as the baseline for its regulatory expectations.

4. Permitted Payment Methods

4.1 Categories of Permitted Payment Methods

The Company accepts player deposits and processes withdrawals exclusively through the following categories of regulated digital payment methods:

- Debit and credit cards (Visa, Mastercard) processed via licensed card-acquiring PSPs
- Open banking / account-to-account (A2A) transfers via licensed open banking providers
- E-wallets operated by FCA-regulated or equivalent entities
- Player-attributed payment wallet instruments approved by the Company under Section 3.2, treated as e-wallet equivalents
- Prepaid vouchers issued by regulated PSPs, subject to the cash-equivalent conditions in Section 3.2
- Bank transfers via IBAN/SEPA rails intermediated by licensed payment processors
- Cryptocurrency, subject to the full AML/CFT framework set out in the Company's Cryptocurrency Risk Policy

4.2 Closed-Loop Withdrawal Principle

The Company applies a closed-loop withdrawal principle where operationally possible, returning player funds to the same payment method used for deposit or to a verified account in the player's own name. This is a core AML control designed to reduce the risk of layering through payment method substitution.

Where a player's original deposit method is unavailable for withdrawal (for example, where a card has expired, a voucher instrument cannot receive withdrawals, or a payment method does not support outbound transfers), the Payments team will route the withdrawal to an alternative verified account in the player's name, following Compliance approval. Payments to third-party accounts — accounts not registered in the player's own verified name — require prior MLRO approval and are subject to enhanced due diligence. All such exceptions are logged and reported to the MLRO.

4.3 Third-Party Deposit Handling

The Company takes all reasonable steps to prevent deposits originating from payment accounts not registered in the player's own name. Where a third-party payment is identified, the deposit is quarantined, the player account is placed on hold, and the Compliance Officer is notified immediately. The deposit is returned to the originating account following MLRO review. Where the circumstances give rise to suspicion of money laundering or terrorist financing, the MLRO will file an Unusual Transaction Report (UTR) with FIU Curaçao via the goAML portal.

5. Agency Intermediaries and Payment Service Providers

5.1 Definition

An “agency intermediary” for the purposes of this Policy is any third party that acts as an agent, sub-agent, or intermediary in the collection, transmission, conversion, or disbursement of player funds on behalf of the Company. This includes PSPs, e-wallet operators, open banking providers, card acquirers, voucher processors, and cryptocurrency VASPs.

The Company does not engage natural persons (individuals) as cash-handling agents for the collection or delivery of player funds under any circumstances.

5.2 Contracted Intermediaries

The following table sets out the Company's contracted payment intermediaries as at the effective date of this Policy. All intermediaries are subject to the due diligence requirements in Section 5.3.

Provider	Type	Function
Bitpace	Cryptocurrency PSP (VASP)	Crypto deposits and withdrawals
MiFinity	E-wallet / Bank transfer	Deposits, withdrawals, crypto wallet, Virtual IBAN
Paysage (Golden Rain Finance Ltd)	Card acquiring	Card deposits
GumBallPay	Card acquiring	Card deposits
Citizen / Yaspa	Open banking	Deposits and withdrawals
Flexepin	Prepaid voucher PSP	Deposits only
Utorg	Paysafecard gateway	Voucher deposits
Skrill / Neteller (Paysafe)	E-wallet	Deposits and withdrawals
MuchBetter	E-wallet	Deposits and withdrawals
Impaya	Card / Open banking	Card deposits
PaymentIQ (GiG)	Payment orchestration	Payment routing and fraud rules — all rails

5.3 Intermediary Due Diligence

Prior to engaging any new intermediary, and on an ongoing basis thereafter, the MLRO must conduct and document: verification of the intermediary's regulatory licence or registration; review of its AML/CFT policies, procedures, and controls; assessment of its sanctions screening and transaction monitoring capabilities; confirmation of Travel Rule compliance where applicable (FATF Recommendation 16); PEP and sanctions screening of UBOs and key principals; review of contractual compliance obligations including data protection and audit rights; and annual re-screening and relationship review.

Intermediaries domiciled in or operating from FATF high-risk or non-cooperative jurisdictions are prohibited unless the MLRO documents a specific risk assessment and the Board approves the exception in writing.

5.4 Intermediary Contractual Requirements

All intermediary contracts must include provisions requiring the intermediary to: apply AML/CFT controls at or above the standard required by this Policy; comply with applicable sanctions obligations and screen against OFAC SDN, UN, and EU lists; notify the Company immediately of any regulatory action, licence suspension, or material compliance breach; permit the Company or its nominated auditor to inspect compliance records on reasonable notice; and not sub-contract the handling of Company player funds to an unlicensed or unregistered entity.

5.5 Payment IQ — Payment Orchestration

All payment flows are routed through PaymentIQ (PIQ), the payment orchestration and fraud-rules platform. PIQ is not a PSP and does not hold player funds; it routes transactions between the Company's cashier and the contracted PSPs listed in Section 5.2. PIQ applies configurable fraud rules and transaction limits as directed by the business.

6. AML Controls Specific to Payment Channels

6.1 Transaction Monitoring

The Company's transaction monitoring system covers all payment channel activity: deposit via a cash or cash-equivalent method not on the permitted list; deposits from payment accounts not matching the player's verified identity; rapid deposit-withdrawal cycles with minimal gaming activity; multiple payment methods used across a single account within a short period; deposits at or just below the NAf. 5,000 NORUT reporting threshold (structuring indicators); and any payment routed via an intermediary not on the Company's approved list.

6.2 CDD and Reporting Thresholds

Obligation	Threshold	Trigger	Required Action
Customer Due Diligence (NOIS)	NAf. 4,000 cumulative (~EUR 2,000)	Cumulative player transactions reach threshold	Full CDD — identity verification, source of funds, risk classification. Internal alert at NAf. 2,000.
Unusual Transaction Report (NORUT)	NAf. 5,000 per transaction (~EUR 2,500)	Single transaction at or above threshold	Mandatory UTR filed with FIU Curaçao via goAML within 48 hours. Objective trigger — no suspicion required.

6.3 Voucher and Prepaid Instrument Controls

Voucher-based deposits (currently Flexepin) present elevated risk of anonymous funding. The following controls apply:

- The player must be the registered holder of the voucher PIN;
- Voucher deposits are subject to a lower EDD trigger threshold than card or bank transfer;
- Withdrawals cannot be processed to a voucher instrument — the Payments team must route to a verified bank or card account;
- Where a player deposits exclusively via voucher and cannot provide a verified bank or card account for withdrawal, the account is placed under compliance review; and
- Repeated or high-volume voucher deposits are escalated to the MLRO.

6.4 Cryptocurrency Payment Controls

Cryptocurrency deposits are converted to fiat at the point of receipt by the contracted VASP. The fiat equivalent is credited to the player's account balance. The Company does not hold cryptocurrency on behalf of players. All cryptocurrency controls, including blockchain analytics screening, wallet attribution requirements, and the same-wallet withdrawal rule, are set out in full in the Cryptocurrency Risk Policy and are applied in conjunction with this Policy.

6.5 Record Keeping

All payment channel records are retained for a minimum of five years from the date of the transaction, or five years after the business relationship ends, whichever is later. Records include all deposit and withdrawal transaction records, PSP settlement statements, intermediary due diligence files, Payment IQ fraud-rule logs, third-party payment exception records, UTR filings, and MLRO decision logs. Records are maintained in a secure, auditable format and made available to the CGA or FIU Curaçao upon lawful request.

7. Governance and Accountability

Role	Responsibility
MLRO / Compliance Officer (Kameshni Chetty)	Owns and annually reviews this Policy. Approves onboarding of new intermediaries. Reviews KYB due diligence files. Approves exceptions to the closed-loop withdrawal principle. Oversees PIQ fraud-rule configuration. Files UTRs with FIU Curaçao.
Payments Team (Head: Dominik Kocka)	Day-to-day operation of the PIQ platform. Monitoring of PSP performance and availability. First-line review of flagged transactions. Ensures withdrawal routing complies with the closed-loop principle.
Board of Directors	Approves this Policy and the Business Risk Assessment. Receives periodic updates on payment channel risks and intermediary landscape. Approves exceptions to the FATF high-risk intermediary prohibition. Formally adopts any material amendments.

This Policy is reviewed annually or whenever there is a material change to the Company's payment methods, intermediary arrangements, or CGA regulatory requirements. Amendments are approved by the Board and communicated to all relevant personnel.

8. Breach of Policy and Escalation

Any actual or suspected breach of this Policy — including any attempt to introduce cash into the payment ecosystem, any unauthorised intermediary arrangement, or any payment routed via an unapproved channel — must be reported to the MLRO immediately. The MLRO will assess the breach, determine whether CGA notification is required, and implement remediation.

Where a breach involves a suspected money laundering or terrorist financing offence, the MLRO will file a UTR with FIU Curaçao without delay via the goAML portal.

Employees who fail to comply with this Policy are subject to disciplinary action up to and including termination. Third-party intermediaries who breach their contractual compliance obligations are

subject to immediate contract review and potential termination. Whistleblower protections apply to any person making a good-faith report under this Policy.

9. Version Control

Version	Date	Changes
1.0	June 2026	Initial Draft
2.0	July 2026	Broadened scope as group policy and aligned with Group AML/CFT policies