

Crypto Asset Policy

Olympus Holdings N.V.

Effective Date: 01.08.2025

Next Review Date: 01.08.2026

1. Introduction

Olympus Holdings N.V. ("Olympus"), operating online gaming platforms including www.fireslots.bet and www.casinoempire.com, is committed to maintaining the highest standards of integrity, compliance, and financial transparency. This Crypto Asset Policy governs the use, acceptance, monitoring, and oversight of cryptocurrencies within Olympus' gaming operations.

This Policy is implemented under Curaçao's AML/CFT and online gaming regimes:

- **LOK** – *Landsverordening op de kansspelen* (Online Gaming Ordinance) establishing the **Curaçao Gaming Authority (CGA)** as supervisor.
- **LID** – *Landsverordening identificatie bij dienstverlening* (Customer identification).
- **NORUT / LMOT** – National Ordinance on the Reporting of **Unusual Transactions** (objective/subjective indicator regime) and associated decrees.
- **FIU Curaçao** – Receipt of **Unusual Transaction Reports (UTRs)** via **goAML**.
- **International Standards:** FATF Recommendations (incl. virtual assets), EU best practices on VASPs and sanctions.
- The **Financial Action Task Force (FATF)** Recommendations;
- EU regulations on virtual asset service providers (VASPs);
- Olympus' internal **Anti-Money Laundering (AML)/Counter-Terrorism Financing (CTF)** program.

Terminology: "Suspicious transactions" are **not** used in Curaçao law. Olympus uses **Unusual Transactions (UTRs)** consistent with NORUT/LMOT.

2. Scope

This policy applies to:

- All Olympus customers engaging in deposits or withdrawals using cryptocurrency;
- Olympus employees responsible for onboarding, compliance, and operations;
- Third-party service providers facilitating crypto processing, custody, or analytics.

3. Definitions & Abbreviations

- **CGA:** Curaçao Gaming Authority (sector supervisor).
- **FIU:** Financial Intelligence Unit Curaçao (receives UTRs via goAML).
- **UTR:** Unusual Transaction Report (objective/subjective indicators).
- **CDD/EDD:** Customer Due Diligence / Enhanced Due Diligence.
- **KYW:** Know-Your-Wallet (ownership and risk of customer wallet).
- **KYT:** Know-Your-Transaction (blockchain analytics).
- **VASP:** Virtual Asset Service Provider.
- **goAML:** FIU reporting portal.

4. Roles & Responsibilities

- **Board of Directors:** Ultimate accountability for crypto risk; approves Policy and major changes.
- **Compliance Officer / MLRO:** Day-to-day AML/crypto compliance; UTR decisions; liaison with FIU/CGA; maintains registers and QA program.
- **Compliance Team:** Performs CDD/EDD, KYW/KYT, monitoring, case management, sanctions screening, UTR preparation.
- **Operations/Payments:** Enforces wallet whitelists; blocks restricted flows; executes holds/freezes as directed by Compliance.
- **IT/Security:** Implements geoblocking, IP/VPN controls, data retention, and system access controls.
- **All Staff:** Complete training; escalate red flags; adhere to no-tip-off rules.

3. Permissible Use of Crypto Assets

Olympus may accept and process cryptocurrency transactions for:

- Deposits into verified player accounts;
- Withdrawals to verified wallets;
- Promotional or loyalty purposes (subject to compliance approval).

Only the following cryptocurrencies may be accepted initially (subject to periodic review):

- Bitcoin (BTC)

- Ethereum (ETH)
- USDT (Tether) on approved chains (e.g., ERC-20, TRC-20)

4. Onboarding and Verification Requirements

All customers wishing to deposit or withdraw via crypto must:

- Complete **full Customer Due Diligence (CDD)** including proof of identity, residence, and source of funds;
- Register a personal cryptocurrency wallet in their own name;
- Undergo **wallet verification** via signed message or third-party validation;
- Undergo **PEP, sanctions, and adverse media screening**.

Cryptocurrency transactions will only be processed if the customer's profile is verified and approved by the Compliance team.

5. Source of Funds and Wealth for Crypto

Customers must demonstrate the legitimate origin of their crypto assets. Acceptable documentation includes:

- Crypto trading account statements
- Mining income records
- Payslips, tax returns, or bank statements showing fiat-to-crypto conversions

Olympus reserves the right to deny transactions if the source cannot be reasonably verified.

6. Blockchain Analysis and Risk Scoring

Olympus shall employ third-party blockchain analytics solutions (e.g., Chainalysis, Elliptic) to:

- Screen all wallet addresses for links to illicit sources (e.g., darknet markets, mixers, ransomware);
- Assign a **risk score** to each incoming and outgoing crypto transaction;
- Detect structuring, layering, or unusual transaction patterns.

Transactions deemed high-risk will be flagged for **manual MLRO review** and may be frozen pending investigation.

7. Transaction Monitoring and Thresholds

Crypto transaction monitoring is integrated into Olympus' AML system. Key thresholds:

- **€2,000**: Trigger alert and log source of funds
- **€5,000+**: Require enhanced due diligence (EDD)

- **Rapid in-and-out** transactions within 24 hours: Automatic review

All unusual transactions (UTRs) will be escalated to the Money Laundering Reporting Officer (MLRO) and reported to the Curacao Financial Intelligence Unit (FIU) where required.

8. Record-Keeping and Retention

Olympus shall retain the following for a minimum of five (5) years:

- Crypto transaction logs and wallet addresses
- CDD and EDD documents
- Blockchain analysis results
- unusual transaction (UTR) reports

All records must be accessible for audit and regulatory inspection.

9. Third-Party Crypto Service Providers

Olympus may engage regulated or reputable crypto payment processors or wallet service providers. All such providers must:

- Undergo initial and ongoing **KYB (Know Your Business)** due diligence;
- Maintain a license or registration where applicable;
- Contractually agree to Olympus' AML and data protection standards.

10. Sanctions Compliance

Olympus will screen all crypto-related parties and wallets against sanctions lists including:

- OFAC SDN list
- EU and UN consolidated lists
- OFSI (UK)
- National and FATF high-risk jurisdictions

Any match or suspicion will result in **immediate escalation**, account suspension, and reporting.

11. Training and Awareness

Staff involved in crypto operations shall undergo specialized AML and crypto risk training annually, including:

- Virtual asset typologies
- FATF red flags

- Blockchain analytics tools and interpretation

12. Governance and Oversight

The **Board of Directors** is ultimately responsible for crypto risk oversight. Day-to-day compliance is managed by the **MLRO**. The policy will be reviewed annually or in response to:

- Changes in regulation or law
- Introduction of new crypto products or payment channels
- Material changes in risk exposure

Terminology: references in this Policy to “suspicious transactions” are replaced by “unusual transactions (UTRs)” as defined by Curaçao law. Reporting is made to FIU Curaçao via goAML without delay.

13. Objective Indicators and Thresholds (UTR Triggers)

In addition to the firm’s internal risk thresholds, the following Curaçao-specific objective indicators apply and trigger UTR filing irrespective of internal risk scores:

- Cash-in/cash-out, deposit, withdrawal or wager flows meeting or exceeding NAF 5,000 in a single gaming day for a customer (aggregated per day).
- A sanctions-list match (UN/EU/Kingdom sanctions) or a positive match against any mandatory screening list.

Internal thresholds (e.g., alerts from €2,000; EDD from €5,000) remain in force as risk controls, but they do not replace the legal objective indicators above.

14. Unusual Transaction Reporting (UTR) and goAML Process

- Registration: Olympus must maintain an active goAML organization account with FIU Curaçao, with designated MLRO and Compliance Officer users.
- Escalation: Analysts escalate candidate UTRs to the Compliance Officer/MLRO using the Case Management workflow; the MLRO makes the final determination.
- Timelines: UTRs must be filed without delay once objective/subjective indicators are met; the decision, rationale, and date/time are recorded.
- Content: UTR submissions must include customer identifiers, transaction details (hashes/addresses for on-chain activity), reasons/indicators, and supporting documents.
- Record-keeping: Retain goAML submission receipts/acknowledgements and evidence for at least 5 years from the date of filing.

- Post-filing actions: Where sanctions are involved, block/freeze as legally required and do not tip-off the customer.

15. Sanctions Screening and Response

- Screen against UN, EU, and applicable Kingdom of the Netherlands sanctions lists; include local implementation measures applicable in Curaçao.
- A confirmed sanctions match constitutes an objective indicator: file a UTR and apply freezing/blocking measures as required by law.
- Document false positives with clear rationale; maintain a sanctions-hit register.

16. Compliance Officer (CGA) Duties

- Independence: The Compliance Officer reports to the Board/Risk Committee and has unimpeded access to data, staff, and systems.
- Training: Maintain and deliver annual AML/CFT and crypto-specific training; track completion; ensure role-specific competence.
- Monitoring & Registers: Maintain UTR register, sanctions-hit register, PEP/adverse-media registers, and audit trails of case handling.
- Reporting: Provide periodic AML/CTF reports to senior management and CGA as required; coordinate with FIU Curaçao for feedback and outreach.
- Quality Assurance: Quarterly sampling of KYC, EDD, blockchain analytics decisions, and UTR filings to ensure consistency.

17. Crypto Controls (VASPs, Travel Rule, and Blockchain Analytics)

- Only engage third-party payment processors and exchanges that are licensed/registered Virtual Asset Service Providers (VASPs) in their jurisdictions and Travel Rule compliant.
- Collect/verify customer wallet ownership (KYW) and risk-score external addresses before first use; block mixers, darknet services, sanctioned wallets, and high-risk typologies.
- Maintain on-chain evidence (TXIDs, addresses, screenshots/reports) with case files for at least 5 years.
- If Olympus ever provides custody or transfer services, obtain all required approvals and expand controls accordingly before go-live.

18. Customer Onboarding (CDD/EDD)

Customers using crypto must:

1. Complete **CDD** (government ID, verification of residential address).
2. Provide **Source of Funds/Source of Wealth** appropriate to risk (e.g., exchange statements, mining income records, paystips/tax returns evidencing fiat-to-crypto conversions).
3. Undergo **PEP, sanctions, and adverse media** screening at onboarding and on a continuous basis.
4. Register **personal wallet(s)** and complete **KYW** (see §9).

Denial: Olympus may refuse crypto activity where SoF/SoW cannot be reasonably verified or risk cannot be mitigated.

19. Know-Your-Wallet (KYW) & Wallet Verification

- **Ownership proof:** Signed message from the wallet (where supported), micro-transaction return test, or third-party verification acceptable to Compliance.
- **Whitelist:** Only **verified wallets** may transact. Changes trigger **EDD** and a **24–48h cooling-off** (configurable by MLRO).
- **Prohibited:** Custodial wallets that cannot evidence customer ownership; wallets linked to mixers, tumblers, darknet services, sanctioned entities, child sexual abuse material (CSAM) typologies, ransomware, or other high-risk categories.

20. Third-Party Providers (VASPs, Processors, Analytics)

- Engage only **licensed/registered** VASPs/processors; document KYB, AML controls, and **Travel Rule** capability.
- **Travel Rule:** Olympus fulfills Travel Rule expectations through its regulated processors; where originator/beneficiary data is provided, Olympus **collects, stores, and reconciles** this with customer records.

- Use reputable **blockchain analytics** (e.g., Chainalysis/Elliptic) for address and transaction risk scoring.

21. Sanctions & Jurisdictional Controls

- Screen **customers, counterparties, and wallets** against **UN, EU, Kingdom of the Netherlands** (and other applicable) sanctions lists at onboarding and prior to each payout.
- **Geoblocking:** Deny access from sanctioned or otherwise prohibited geographies; enforce via IP checks, device fingerprinting, payment controls, and document checks.
- **Action on hits:** **Freeze/block** as legally required; **file a UTR** (objective indicator where applicable); **no tipping-off**.

22. Blockchain Analytics (KYT) & Risk Scoring

- **All inbound/outbound addresses** screened before first use and on a rolling basis.
- **Risk bands (reference values; MLRO may adjust):**
 - *Low (0–24):* Auto-allow; routine monitoring.
 - *Medium (25–49):* Allow with SoF note; increase monitoring.
 - *High (50–74):* Manual review; require EDD and MLRO approval.
 - *Severe (≥ 75 or prohibited category):* Block/freeze; escalate; consider UTR.
- **Pattern detection:** Structuring, chain-hopping, rapid in-and-out ($\leq 24h$), newly created wallets with large flows, interaction with high-risk services, abnormal velocity or frequency.

23. Transaction Monitoring & Thresholds

Internal, risk-based controls (for alerting/escalation):

- **€2,000 (aggregate daily):** Create alert; record/update Source of Funds note.
- **€5,000 (aggregate daily or single transfer):** **EDD** required prior to further activity.
- **Rapid in-and-out $\leq 24h$** or multiple near-threshold deposits: Automatic review.

*These internal thresholds do **not** replace Curaçao's legal objective indicators below.*

24. Curaçao Objective & Subjective Indicators (UTR Triggers)

24.1 Objective Indicators (file UTR irrespective of internal risk score)

- **NAf 5,000** (cash or cashless) **in a single gaming day per customer** (aggregated) across deposit/withdrawal/wager flows.
- **Positive sanctions-list match** (UN/EU/Kingdom or mandated lists).

24.2 Subjective Indicators (examples – file UTR where warranted)

- Use of mixers/tumblers; ransomware or darknet linkages; service category “extremes.”
- Deposits from/to third-party wallets; unexplained chain-hopping; mule indicators.
- Customer behavior inconsistent with profile/SoF; refusal to provide KYW/SoF evidence.
- Multiple accounts, VPN evasion, or geolocation contradictions.

25. UTR Reporting via goAML (FIU Curaçao)

- **Registration:** Maintain active **goAML** organization account; designate users (MLRO, deputies).
- **Escalation:** Analysts escalate candidate UTRs to MLRO via Case Management; MLRO makes final determination.
- **Timelines:** **File without delay** once an objective/subjective indicator is met.
- **Content:** Include customer identifiers, transaction details (TXIDs, hashes, addresses), reasons/indicators, sanctions/KYT results, and supporting documents.
- **Post-Filing Actions:** Where sanctions involved, **block/freeze** as required; **no tipping-off**; document all decisions.
- **Evidence:** Retain goAML submission receipts/acknowledgements and working papers in the **UTR register**.

26. Records & Data Retention

Maintain for **at least 5 years** (longer if required by law or investigation):

- CDD/EDD/KYW/KYT files; wallet whitelists and changes; processor due-diligence files.
- Transaction logs (on-chain TXIDs, addresses), analytics reports/screenshots.
- UTR filings and FIU acknowledgements; sanctions-hit and PEP/adverse-media registers.
- Monitoring alerts, cases, decisions, and QA samples.

27. Training & Awareness

- **Annual AML/CFT & crypto-specific training** for all relevant staff, including FATF red flags, Curaçao UTR regime, blockchain analytics, sanctions, and no-tip-off obligations.
- **Role-specific** upskilling for analysts and MLRO; training completion tracked.

28. Governance, QA & Registers

- **Registers:** UTR register; sanctions-hit register; PEP/adverse-media register; wallet whitelist/exceptions; training register; processor/VASP due-diligence register.
- **Quality Assurance:** Quarterly sampling of KYC/EDD, KYW/KYT decisions, sanctions handling, and UTR filings for consistency; report findings to the Board/Risk Committee.
- **Management Reporting:** Periodic AML/crypto risk reports to senior management and CGA as requested.

29. Security & Operational Controls

- **Access controls & audit trails** for monitoring systems and wallet-whitelist management.

- **Incident response:** Documented procedure for freezes/holds, account suspension, evidence preservation, and regulator/FIU engagement.
- **Business continuity:** Ensure alternate FIU reporters and system redundancies.

30. Change Control & Policy Review

- Monitor **CGA circulars/rulings**, FIU indicator updates, FATF guidance, and processor changes.
- **Review within 30 days** of any material change (regulatory or risk).
- Log revisions in a **Version History** (date, description, approver) and communicate updates to staff.

31. Currency & FX Handling

- Curaçao legal **objective thresholds are assessed in NAf (ANG)**.
- Internal alert thresholds may be set in **EUR**; Compliance must maintain documented **FX conversion** logic and staff guidance to avoid confusion.

32. Jurisdictional Controls and Geoblocking

- Deny access from sanctioned countries/territories and other prohibited geographies; enforce using IP geofencing, payment controls, and document checks.
- Where residency or source-of-funds contradictions arise (e.g., VPN usage), trigger EDD and pause transactions pending resolution.

33. Change Control and Regulatory Monitoring

- Monitor CGA circulars/rulings and FIU Curaçao indicator updates; review and update this Policy within 30 days of any material change.
- Log all revisions in the Document Control register (version, date, approver) and communicate updates to staff.

34. Risk Assessment Linkage

- Reference Curaçao's National Risk Assessment (latest available) in the firm's enterprise AML risk assessment; map identified crypto-related threats and vulnerabilities to control design and monitoring intensity.

35. Exceptions

- Any exception to this Policy requires **documented MLRO approval** and, where material, **Board** acknowledgement. Exceptions must be time-bound and captured in the **exceptions register**.

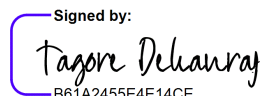
36. Enforcement

Violations may result in account restriction/closure, employee disciplinary action, or regulatory reporting, as applicable.

Approved by:

Board of Directors, Olympus Holdings N.V.

Date: 01.08.2025

Signed by:

B61A2455E4E14CE...