MAY PAYMENT SP. Z O.O. SUSPICIOUS TRANSACTION REPORTING POLICY

Policy Name	Suspicious Transaction Reporting Policy	Version	2.0.
Drafted by	Internal legal and compliance team, strictly confidential and this information can be provided by the official request by the third party (Regulator, External Provider and/or Client)	Approved by Board on: 01.01.2026	
Responsible person	Internal legal and compliance team, strictly confidential and this information can be provided by the official request by the third party (Regulator, External Provider and/or Client)	Scheduled review date: 30.12.2026	

INTRODUCTION

This **MAY PAYMENT Sp. z o.o.** (hereinafter referred to as "**May Payment**", "**our business**", "**Company**" "**we**", "**our**" or "**business**") Suspicious Transaction Reporting Policy (hereinafter referred to as " **Policy**") establishes comprehensive procedures for detecting, documenting, escalating, and reporting suspicious transactions and other illicit financial activity at Company, a Polish-licensed Virtual Asset Service Provider (VASp/CASP). It applies to all business units (exchange, wallet, ICO platform, staking) and all employees, officers, and directors. The Policy aligns with Polish AML/CFT law (Act of 1 March 2018), GIIF (General Inspector of Financial Information) guidelines - https://www.gov.pl/web/finance/aml-cft, Polish Financial Supervision Authority rules, the EU Markets in Crypto-Assets (MiCA) regulation, FATF recommendations- https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-fur/Poland-MONEYVAL-FUR-2024.pdf.coredownload.inline.pdf, ISO/IEC 27001 - https://www.iso.org/standard/27701?utm_source=google&utm_medium=ppc_paid_social&utm_campaign=ISO27701&utm_content=gads01&gad_source=1&gad_campaignid=23119986168&gbraid=0AAAAABtQACHnc5mmY1XipIidjBPyApIGh&gclid=CjwKCAjw04HIBhB8EiwA8jGNbf2SdmI9XE8x7GUHNqKhYn-sLbMXw0uCkvn6xXTHRsOOq09sUiy2OhoCYcMQAvD_BwE. information security controls, and other applicable EU AML/CFT regulations. Its objectives are to ensure prompt identification of red flags, effective internal reporting to the AML Officer/MLRO, timely external reporting to GIIF, and robust record-keeping and security controls.

I. REGULATORY FRAMEWORK

1. Polish AML Act (2018) https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.gov.pl/attachment/8a157019-cbbc-44bd-8079-2522f342b997&ved=2ahUKEwi34oq6msyQAxXcB9sEHZmPDRsQFnoECBoQAQ&usg=AOvVaw3WqFT5tqaGvJRZa-2Wprb4: Under Art. 74, any "obligated institution" (including VASPs) should notify GIIF of "any circumstances which may indicate the suspicion of committing the crime of money laundering or terrorist financing". Reports ("suspicious transaction reports", STRs) should be submitted immediately and in any case within 2 business days of confirming a suspicion. Article 72 requires reporting to GIIF of large transactions: accepted payments or withdrawals exceeding EUR 15,000, executed transfers over EUR 15,000, and foreign currency exchanges over EUR 15,000. Such threshold reports should be submitted within 7 days of the transaction. Article 86 provides for immediate notification and optional freezing of a transaction if there is a "justified suspicion" before its execution. Documentation retention (customer ID, transaction records, STR analyses) should comply with the law (e.g. retain relevant records for at least 5 years).
2. GIIF/FIU Requirements- https://www.gov.pl/web/finance/aml-cft: GIIF is Poland's financial intelligence unit. GIIF's decision of 28 Sept. 2023 requires VASPs to submit quarterly AML reports via the GIIF ICT system. But more critically, GIIF requires immediate STR reporting via its secure electronic portal. Reports should be e-signed with a qualified signature. GIIF may respond with a freeze request (Art. 86) or share analysis with prosecutors.
3. MiCA (EU Reg. 2023/1114): MiCA defines "Crypto-Asset Service Providers" (CASPs) and mandates robust governance and compliance programs. While MiCA itself defers to national AML law, it underscores the need for CASPs to have AML controls, customer due diligence, transaction monitoring, and reporting mechanisms. EU supervisors (ESMA, NCAs) emphasize that licensed CASPs should implement AML/CFT procedures and cooperate with FIUs under national law.
4. FATF and EU AML Standards: Globally, FATF Recommendation 15 (new technologies) and R20/R16 (travel rule) require VASPs to apply risk-based AML controls, CDD, and timely STR reporting to FIUs. The EU's 5th/6th AML Directives similarly impose STR obligations on crypto-asset service providers. This Policy incorporates FATF red-flag indicators and EU best practices.
5. ISO 27001 Information Security: This Policy integrates ISO/IEC 27001:2022 requirements. Information and systems used for AML should be protected by access controls (Annex A.5/A.9: least privilege, RBAC). All security events, transaction reviews, and user actions should be logged and auditable (Annex A.8.15/A.12: logging of access attempts, data access, system changes). An incident response plan (Annex A.16) should exist for cybersecurity or process breaches, ensuring swift, documented handling of any AML-related incident.

II. ROLES AND RESPONSIBILITIES

1. **Board of Directors/Management** – They approve and review this Policy, ensure adequate resources (staff, technology, training) for AML compliance, set a "no tolerance" tone for money laundering. Please see herein the Key Personnel of the Company:

Key Personnel:

Mrs. Oksana Dranenko - Director at May Payment sp z.o.o (May Payment)
LinkedIn link – https://www.linkedin.com/in/oksana-dranenko-811942346/

Head of Legal and Compliance Department at May Payment sp z.o.o (May Payment)
https://docs.google.com/document/d/1rnLZ1VOmJ2YSGB9K87qNS4mGKennLKmp/edit

Head of Technical Support Department at May Payment sp z.o.o (May Payment)
https://docs.google.com/document/d/1ig_1Rt5HLWby08dH30OH8qpFxFIYZeUyxJIkbDvZLZ8/edit?tab=t.0

Anti-Money Laundering and AML Officer/MLRO Officer (AML reporting and risk compliance)

Our CEO of May Payment sp z.o.o (May Payment) Mrs. Oksana Dranenko is a highly experienced professional who possesses good knowledge and skills in business formation, business growth and development, strategy making and implementation, sales, business analytical skills and product development. Mrs. Oksana Dranenko is a great in line manager including performance management, motivation of staff, team building and delivering objectives within agreed timescales.
The professional experience of Mrs. Oksana Dranenko includes 1 (one) year of leading business operations of May Payment sp z.o.o for several month. Mrs. Oksana Dranenko has been a shareholder and managing director of several businesses in finance, MSB and other related areas as well in several jurisdictions.
Mrs. Oksana Dranenko has been leading May Payment sp z.o.o as the Shareholder and Director since September 2025 as a director, the director's main responsibilities consist of:

- developing and ensuring the execution of company's business plans;
- designing business development strategy;
- analyzing problematic situations and occurrences and provide solutions to ensure company survival and growth;
- delegating responsibilities and supervising the work of executives;
- providing guidance and motivation to drive maximum performance;
- Identifying and establishing sales leads and following up with approaches to appropriate target clients.

III. CUSTOMER DUE DILIGENCE AND RISK ASSESSMENT

1. **Know Your Customer (KYC/KYB):** Before onboarding, we verify customer identity and beneficial ownership per legal standards (ID documentation, verifying source of funds). We assign a risk rating based on customer type, geography, occupation, source of wealth, expected transaction size/frequency, and product type (e.g. an ICO participant or institutional staking client may have higher risk). Enhanced due diligence (EDD) is applied for high-risk customers (e.g. PEPs, sanctioned entities, complex ownership).
2. **Periodic Review:** Customer profiles and risk ratings should be reviewed periodically (at least annually or triggered by new information). We systematically update KYC data when changes occur (big transactions, change of occupation, address, etc.).
3. **Transaction Monitoring:** We implement automated monitoring of transactions and account activity. Configurable alerts flag transactions based on risk rules (e.g. thresholds, velocity, destination). Examples: large crypto transfers to unknown addresses, rapid self-to-self transfers, new wallet funding, pattern anomalies. The system reflects the red flags listed below.
4. **Risk Assessment:** We perform a comprehensive AML/CFT risk assessment for the business and specific products/channels. We document inherent risks (e.g. wallet transfers, overseas trading) and mitigating controls. We update the risk assessment whenever there are material changes in products or regulation. The results inform transaction monitoring rules and CDD levels.

IV. IDENTIFYING SUSPICIOUS ACTIVITY

4.1 General Red Flags

1. **Unusual Customer Behavior:** Transactions inconsistent with known profile or business purpose (e.g. a low-income individual making large trades). Sudden changes in activity (high-value trades after a long dormancy). Reluctance or refusal to provide information, or use of complex structures without justification.
2. **Structuring/Smurfing:** Breaking large sums into multiple smaller transactions (just under thresholds) that lack economic rationale. Multiple small deposits or withdrawals from the same customer in a short period.
3. **Rapid Transactions:** Funds quickly entering and exiting wallets or accounts without intended holding. For example, a customer's wallet is funded and then entirely drained within minutes, then refunded from another source (a pattern indicative of layering).
4. **Cross-Border Dynamics:** Transactions routed through multiple jurisdictions, especially to or from high-risk/low-AML regions (e.g. countries on FATF grey or blacklists). Multiple transfers in quick succession to foreign exchanges or casinos, without clear purpose.
5. **Use of Multiple VASPs:** Immediate or rapid transfers of funds to several different crypto exchanges/VASPs, especially where the customer has no known business in that jurisdiction. Transfers to little-known VASPs or mixers/tumblers (see below).

6. The above indicators are not exhaustive. A combination of factors or any unexplained unusual pattern should heighten scrutiny.

4.2 Crypto-Specific Red Flags

1. **Mixers/Tumblers:** Use of anonymizing services (e.g. Tornado Cash, CoinJoin) to obfuscate transaction origin. For example, promptly withdrawing crypto from our platform to an external wallet and then exchanging it via a mixer – "effectively turns the VASP into a money laundering mixer".
2. **Chain-Hopping and Privacy Coins:** Rapidly converting assets across different blockchains, or involving privacy coins (Monero, Zcash) known for untraceability. The use of privacy coins is itself a red flag, as they are "significant" in illicit use.
3. **Peer-to-Peer Transactions:** Large transfers between wallets that bypass the exchange or involve non-custodial addresses, especially if funds flow through multiple wallets in a "peel chain" (layered peeling of funds).
4. **Micro-Transactions (Structuring):** Many small transactions (just below reporting thresholds) in quick succession, aiming to avoid detection.
5. **Funding from Blacklisted Sources:** Deposits from crypto addresses linked to cybercrime (the platform's sanction screening should flag any address on OFAC/EU lists). Accepting funds from addresses already flagged as "stolen" is highly suspicious.
6. **New or Dormant Accounts:** A newly created account that immediately conducts large transactions or repeatedly transfers its entire balance out. E.g., a customer makes a huge initial deposit far exceeding declared means, then tries to withdraw or move funds immediately (an "initial deposit inconsistent with profile" scenario).\
7. **Exchange-Withdrawal Patterns:** Depositing crypto to our platform and quickly withdrawing in a different crypto or fiat currency, without sufficient economic reason (incurring fees without a clear purpose).

V. INTERNAL SUSPICIOUS ACTIVITY REPORTING PROCEDURES

5.1 Detection and Initial Review

1. **Triggering Alerts:** Automated monitoring systems generate alerts based on the criteria above. Front-line staff receiving a transaction or customer interaction that appears suspicious should immediately flag it (e.g. via internal compliance portal, e-mail, or hotline). No employee should attempt to "verify" suspicion without consulting compliance.
2. **Initial Documentation:** The person identifying the potential issue should immediately document relevant facts: customer details, transaction data (amounts, dates, counterparties), and why it appears suspicious (e.g. "transaction pattern inconsistent with prior account usage"). This is entered into a Suspicious Activity Report (SAR) or case file, which should include supporting evidence (screenshots of transaction history, communications, KYC records, etc.).
3. **Escalation to Compliance/AML Officer/MLRO:** The completed SAR and documentation are forwarded without delay to the AML/Compliance department and AML Officer/MLRO. If the AML Officer/MLRO is unavailable, the Deputy AML Officer/MLRO or Head of Compliance handles the case. Staff should not execute or permit the transaction until it has been reviewed (unless delaying a live transaction might tip off the customer).

5.2 Review and Analysis by AML Officer/AML OFFICER/MLRO

1. **Investigation:** The AML OFFICER/MLRO (or designee) reviews all available information (KYC files, transaction records, monitoring alerts, external data) to assess the suspicion. The AML OFFICER/MLRO may query the customer for an explanation or ask for additional documentation, documenting all interactions. The analysis includes checking whether any red flags co-occur (e.g. high-risk country AND rapid transfers).
2. **Decision Criteria:** If the AML OFFICER/MLRO determines there are reasonable grounds for suspicion (even a low threshold per guidance: as soon as "there is reason to suspect"), the case is escalated to Report. If not, the AML OFFICER/MLRO documents the reasoning and either closes the case or monitors it further. AML OFFICER/MLRO's judgment should err on the side of filing if any doubt remains.
3. **Internal Approval:** All STRs should be approved by the AML OFFICER/MLRO or Head of Compliance. The AML OFFICER/MLRO signs off on the decision to file and ensures legal confidentiality of the process.

5.3 Internal Reporting Chain

1. **Reporting Flowchart:** Employee → Compliance Analyst → AML OFFICER/MLRO → Board (as needed).
2. **Documentation:** Each step (alert generation, reviewer findings, approval) is logged. An audit trail of actions, decisions, and communications is maintained in the AML case management system. Changes in the STR status (e.g. escalate, no action, report filed) are timestamped. This ensures traceability and accountability (in line with ISO 27001 logging requirements).
3. **Confidentiality:** Throughout, details of the investigation and the fact of any reporting are kept strictly confidential within the compliance unit (no tipping-off to customers or outside parties).

VI. External Reporting to GIIF (Financial Intelligence Unit)

6.1 Suspicious Transaction Reporting (STR) – Art. 74
1) When to Report: If, after review, the AML OFFICER/MLRO has reason to suspect ML/TF, an STR should be filed with GIIF. Legally, this means "any circumstances which may indicate suspicion" should be reported.
2) Timing: By law the notification is immediate, but no later than two business days after the AML OFFICER/MLRO confirms a suspicion. Best practice is to report as soon as practicable after escalation (ideally within 24 hours).
3) Method: Reports are submitted via GIIF's secure e-FIU portal. Each report should be electronically signed (qualified signature). The report includes: customer identification (per Art.36(1)), details of other parties if known, account numbers (IBAN or crypto wallet as applicable), transaction amounts/currencies, transaction dates, and a narrative justifying the suspicion. Supporting documentation (transaction records, correspondence) should be attached if possible.
4) Acknowledgment: Upon submission, GIIF sends an automatic receipt confirmation with date/time. This receipt should be archived.

6.2 Pre-emptive Notifications – Art. 86 (Freezing Mechanism)
1) Immediate Notification: If suspicion arises before a planned transaction or withdrawal is executed (for example, a customer attempts a large transfer or withdrawal that raises alarms), the VASP should immediately notify GIIF via electronic means (email or portal) under Article 86. This is separate from the STR (Art.74) and focuses on a specific transaction or assets. The notice includes available information about the suspicious transaction and expected execution time.
2) Temporary Freeze: Once GIIF acknowledges receipt (automatically within minutes), the VASP should temporarily stop the execution and other debits on that account for up to 24 hours.
3) GIIF Request: Within that period, if GIIF believes ML/TF is likely, it may send a formal request to suspend the transaction/block the account for up to 96 additional hours. The VASP should comply immediately with GIIF's request.
4) Closure: If GIIF indicates no basis for reporting to prosecutor within 24h, or grants an exemption, the VASP may proceed as normal. Otherwise, GIIF will notify a prosecutor of a suspected crime.
5) Record: Article 86 notifications and any GIIF responses should be documented. Do not inform the customer that a freeze or notice has been issued.

6.3 Threshold Reporting – Art. 72 (Large Transactions)
1) Large Transactions: Independently of suspicion, the VASP should report certain large transactions to GIIF. Specifically:
2) Crypto-to-fiat an fiat-to-crypto as well as crypto withdrawal to external third party fiat providers (or equivalent cryptocurrency withdrawal) > EUR 15,000,
1) Fund transfers/crypto withdrawal > EUR 15,000, and
2) Purchase/sale of cryptocurrency and withdrawal > EUR 15,000.
Such reports are submitted electronically, including unique transaction ID, date/time, parties involved, currency/amount, and transaction type.

1) Timing: These statutory reports should be sent to GIIF within 7 days of the transaction.
2) Format: GIIF provides standardized forms and portal sections for threshold reports ("kwartalna statystyka" for quarterly data) as noted in GIIF's guidance. The AML OFFICER/MLRO or AML team should ensure periodic submission of these reports (via electronic signature).

6.4 Sanctions and Fines

Failing to report STRs or threshold reports as required can lead to severe penalties: administrative fines, license revocation, and criminal charges for the institution and responsible individuals. Staff should understand that non-compliance with Art.74/86 is a serious offense. (Polish law mandates confidentiality of STR filing, breach of which can carry imprisonment.)

VIII. Record-Keeping and Audit Trails

1) Retention of Documents: All documentation relating to AML/CFT should be retained in secure records. This includes customer identification documents, transaction records, KYC data, internal SAR analyses, GIIF reports, and correspondence. Per law, documents and analysis results should be kept for at least 5 years from the end of the business relationship or transaction date (periods may be extended upon GIIF request).
2) Audit Trail: Digital systems should log all user actions related to AML (e.g. changes in customer profiles, generation of alerts, STR submissions). ISO 27001 requires logging of critical events: system access attempts, data access, and use of admin functions. These logs should be protected against tampering and regularly reviewed.
3) Secure Storage: Physical and electronic records should be stored securely. Access to sensitive AML records is limited to authorized personnel only (per ISO Annex A access control). Backups of electronic data should be maintained to prevent loss.
4) Audit Reports: Maintain a register of all STRs filed (date, FIU reference number), plus any follow-up actions (prosecutor referral, transaction blocking). This register aids supervisors (GIIF/KNF) or auditors in oversight.

IX. Information Security Controls (ISO 27001 Alignment)

1. Access Control (ISO A.5/A.9): AML/CFT systems (transaction monitoring, compliance databases, reporting tools) are accessible only to personnel with defined roles. Access reviews are performed regularly to revoke unnecessary privileges. MFA is used for privileged accounts. Segregation of duties is maintained: those who handle transactions are not the same individuals who approve STRs.
2. Logging and Monitoring (ISO A.8.15/A.12): All system activities relevant to AML (e.g. user logins, data queries, creation of cases) are logged with timestamps and user IDs. Logs are reviewed for anomalies (e.g. unauthorized access attempts). Logs are retained per retention Policy and protected from unauthorized change.
3. Incident Response (ISO A.16): Any information security incident (e.g. data breach exposing customer identities or suspicious cases) triggers the company's Incident Response Plan. Roles and procedures defined under ISO 27001 ensure quick containment, investigation, and remediation. The AML OFFICER/MLRO is notified of any cyber incident that could affect AML data, as such incidents might facilitate laundering. Formal lessons-learned reports are created after incidents.
4. Integrity and Confidentiality: Systems should ensure the integrity of STR and transaction data – e.g. by using cryptographic checks or audit controls. Confidential SAR content is encrypted at rest/transit. Disclosure of any STR or related personal data is strictly limited to authorized regulators and law enforcement, per law.

X. Training, Awareness, and Review

1) Staff Training: All relevant employees receive mandatory AML/CFT training at hire and annually thereafter. Training covers money laundering typologies, crypto red flags (e.g. mixers/tumblers, structuring), and reporting procedures. Specialized training is given to AML OFFICER/MLRO/compliance staff on GIIF reporting systems and legal updates. Records of training completion are kept.
2) Policy Review: This Policy is reviewed and updated at least annually or upon major legal changes (e.g. new EU directives, MiCA updates, GIIF guidance). AML/CFT risks and procedures should be reassessed whenever the company launches a new service (e.g. staking protocol).
3) Internal Audit: Periodic audits (by internal or external auditors) verify compliance with this Policy. Audit findings and regulatory feedback are used to improve the AML program.

XI. Summary of Key Procedures (for Staff Reference)

1. Watch for Red Flags: Be alert for unusual patterns – e.g. very rapid or multiple small crypto transfers, use of privacy coins, or deposits/withdrawals without clear reason. Transactions involving mixers/tumblers or darknet-related addresses are especially suspicious.

2. Know Your Customer: Ensure each customer's identity and risk profile are up-to-date. Any transaction inconsistent with a customer's profile (source of funds, stated activity) should be questioned.

3. Escalate Suspicion Immediately: If you suspect money laundering or terrorism financing, do not execute the transaction. Instead, fill out an internal SAR form or alert your supervisor/Compliance right away. Do not mention your suspicion to the customer.

4. AML OFFICER/MLRO Review: The Compliance team will review the case. If confirmed, the AML OFFICER/MLRO submits a Suspicious Transaction Report to GIIF within 2 business days. Even if unsure, better to report early (the threshold for reporting is very low).

5. Use Article 86 Freeze: For transactions still pending that are suspicious, the AML OFFICER/MLRO will notify GIIF immediately under Article 86 and pause the transaction (up to 24–96 hours).

6. Threshold Reporting: Independently of suspicion, report any transaction over EUR 15,000 (or equivalent) to GIIF within 7 days, including all transfers and foreign exchange.

7. Maintain Records: Keep detailed records of all customer IDs, transaction logs, AML investigations, and filed reports for at least 5 years. All compliance actions (reviews, STRs, freezes) should be logged for audit.

8. Follow Security Protocols: Handle all AML documents and systems with strict access control. Log in with your own credentials; do not share accounts. Report any data breach or system problem immediately.

9. Cooperate with Authorities: If GIIF or law enforcement contacts you (requests information or issues a transaction suspension), comply promptly. All reports made (GIIF reference numbers, dates) should be tracked internally.

All employees should follow these procedures. By diligently monitoring and reporting, we protect our customers, comply with Polish and EU law, and uphold the integrity of our crypto services. Consistent application of this Policy meets GIIF expectations and EU MiCA/CFT standards, and helps avoid regulatory sanctions.

XII. Reporting and review

We conduct periodic internal audits of custody operations, security, and AML controls. Findings are reported to senior management with action plans. Key performance indicators (e.g. number of accounts opened, suspicious alerts, security incidents) are tracked monthly by the risk and compliance teams.

As a licensed CASP, we submit all required reports to the national regulator (e.g. client asset records, incident reports) and cooperate with supervisory reviews and inspections. Any major deficiencies or system outages are reported as per regulator deadlines.

This Policy is to be kept up to date to take into account changing circumstances. In this connection, this Policy provided herein will be updated periodically and at least annually on January 1 of each year to reflect any material change to our operations, infrastructure, business or business location(s).
Changes to systems (updates, infrastructure modifications) follow formal change control as per ISO 27002 to prevent inadvertent disruptions. The CMDB (configuration database) records disaster recovery dependencies. Release testing of software includes rollback procedures.

Major system changes or emerging threats (new attack vectors, regulatory changes) trigger plan updates. Internal audit or external review verifies compliance with standards (including, but not limited to, DORA requirements, EBA guidelines) and suggests improvements. We maintain an issues log and track corrective actions. Document control ensures only the latest approved procedures are in use.

This Policy and related policies are updated for new business activities or regulatory updates (including, but not limited to, MiCAR implementation acts, DORA technical standards, NIS2, etc.). Regular training and awareness programs keep staff prepared as per ISO 22301. By continually aligning with ISO 22301, ISO 27001 and industry best practices, the BCP remains robust and up-to-date.

We publish on our website a summary of this Policy's key points (e.g. segregation, custody procedures, reporting). Fee structures and any material risks (including environmental impact of crypto-assets) are transparently disclosed. We maintain a clear complaints handling procedure and client service contacts.