

REGUSHIELD AI AUDIT REPORT

Case Reference: CASE-2026-6982

Case ID: 13

Workflow: crypto_reserve_monitoring

Generated At: 2026-04-19T14:16:34.179Z

Audit Hash: 69bfa52376f0aee800523d5596ff864b5b0661bd885ba75a9b7917f8cbc5d132

RISK MATRIX

Risk Level: critical

Risk Score: 80

Status: flagged

TRANSACTION CONTEXT

Amount: EUR 2400000

Transaction Count (24h): 18

Customer Type: business

Customer Risk Level: high

Route: LT -> DE

Cross-Border: Yes

PEP Flag: No

Suspicious Pattern: No

COMPLIANCE INPUTS

KYC Status: complete

Sanctions Screening: review_required

Source of Funds: verified

AI REASONING

Escalated to critical due to cross-border route, sanctions review issue, high-risk customer profile. Human review and auditor-ready evidence are required before closure.

LEGAL BASIS

- AML6 - High-Risk Factors / Cross-Border Review
- AML / SAR Escalation Logic
- MiCA / Travel Rule Controls
- EU AI Act Art. 13 - Transparency & Explainability
- AVNT / KGK / ISA Audit Readiness

NARRATIVE

This case highlights significant compliance issues within the crypto reserve monitoring framework. With a transaction amount of €2,400,000 involving a business customer from Lithuania to Germany, the elevated risks associated with cross-border transactions are exacerbated by the complexities identified, namely the reserve mismatch and a gap in compliance with the Travel Rule. This necessitates immediate and thorough action to mitigate potential regulatory repercussions.

RECOMMENDED ACTIONS

- Review and enhance customer due diligence for high-risk customers. [immediate / open]
- Accelerate sanctions screening process and document findings [immediate / open]
- Ensure complete compliance with Travel Rule requirements [immediate / open]
- Perform immediate custody reconciliation checks [immediate / open]
- Conduct a detailed investigation into the reserve mismatch [immediate / open]

NOTES

Reserve mismatch and custody reconciliation exception with Travel Rule metadata gap.

END OF REPORT