**JIL Sovereign Technologies, Inc.**
CRYPTOGRAPHIC VERDICT AUTHORITY - PILLAR 4

REPORT IDENTIFIER
**JIL-VR-WI-2026-04-19-D5C4B3A2**
Issued: 2026-04-19 15:03:51 UTC
Completed: 2026-04-19 15:03:51.187 UTC

PILLAR 4 OF 5 - WALLET INTELLIGENCE RISK RECORD

# Cryptographic Verdict Record

Court-Admissible - Independently Verifiable - Tamper-Evident

SAMPLE - FICTITIOUS SUBJECT DATA

## 0 IDENTIFIERS, RETRIEVAL, AND RETENTION

| | |
|---|---|
| **Report ID (this document)** | `JIL-VR-WI-2026-04-19-D5C4B3A2` |
| **Attestation ID** | `ATT-892444-0000007741` |
| **Vendor ID (requester)** | `VND-EXCHG-0013` (Redacted institutional exchange, onboarded 2025-09-03) |
| **Profile ID** | `PRF-WIE-STANDARD-v4.0` |
| **Date Completed** | 2026-04-19 15:03:51.187 UTC (epoch `1776657831.187`) |
| **Storage Location (vendor-controlled)** | Vendor SDV endpoint `sdv://VND-EXCHG-0013.us-west.jil-sdv/`, object key `verdicts/wallet-intel/2026/04/19/JIL-VR-WI-2026-04-19-D5C4B3A2.pdf.sealed`. AES-256-GCM encrypted, vendor-held key. |
| **Content Hash (SHA-256)** | `c3d4e5f67890a1b2abcdef0123456789fedcba9876543210abcdef0123456789` |
| **Retention Period** | **15 years minimum.** Exceeds BSA / FATF / NYDFS / HIPAA requirements. Permanent retention may be elected by vendor. |
| **Retrieval Index (JIL-side)** | Indexed in `trust.verdict_records` + replicated to `verdict_index.clickhouse`. Queryable by report_id, attestation_id, vendor_id, profile_id, date_completed, subject_hash, L1 anchor tx. |
| **Retrieval API** | Authenticated vendors: `GET /api/v1/verdicts/{report_id}`. Courts/regulators: `GET /verify/{report_id}` returns verification metadata without PII; blob retrieval requires vendor consent or court order served on vendor. |

## 1 SUBJECT OF VERDICT

| | |
|---|---|
| **Request Type** | Wallet Intelligence Risk Record (Pillar 4) - Standalone WIE Evaluation |
| **Requesting Party** | Redacted Institutional Exchange Compliance, Request-ID `rq:7d3a:2c1b:0e9f` |
| **Wallet Under Evaluation** | `0x4d5C8b3A9F2e7C1d6B5a4e3D2c1B0A9F8e7D6C5b` |
| **Chain** | Ethereum mainnet (chain-id 1) |
| **Purpose** | Outbound withdrawal approval ($184,500 wUSDC-JIL) |
| **Policy Trigger** | Amount >$100K threshold - standalone WIE evaluation required |
| **Signal Count Applied** | 42 (all WIE signals) |
| **SLA Target** | 200 ms |
| **Actual Latency** | 187 ms |

## 2 TEST PROFILE APPLIED

| | |
|---|---|
| **Profile Name** | `WIE-STANDARD-v4.0` |
| **Profile Description** | Standalone wallet risk scoring. 42 WIE signals only. |
| **Total Catalog Size** | 111 checks (69 FWEA + 42 WIE) |
| **Approved for this Profile** | **42 of 111** checks enabled |
| **Out of Scope (not approved)** | 69 of 111 checks disabled for this profile |

Coverage transparency: both approved and out-of-scope checks are listed in Section 4 for full court defensibility. No hidden checks, no silent omissions.

## 3 APPROVED CHECKS - FULL TEST MATRIX (SECTION 4A)

**42 APPROVED**

Each approved check ran during verdict assembly. Method, source, result, and per-check evidence hash listed below. Individually Ed25519-signed and rolled up into Section 6 Merkle root.

| CHECK ID | TEST NAME | METHOD | SOURCE | RESULT | EVIDENCE HASH |
|---|---|---|---|---|---|
| **WIE-01** | Destination wallet age | Genesis-tx trace + funding attribution | JIL L1 on-chain history | **847 days (LOW RISK)** | sha256:01de...w1w |
| **WIE-02** | Funding source attribution | Recursive source-of-funds trace | JIL attribution-evm + Chainalysis | **CLEAR** | sha256:02fu...w2w |
| **WIE-03** | First-block recency flag | Age vs transaction volume ratio | JIL L1 + chain-specific | **CLEAR** | sha256:03fi...w3w |
| **WIE-04** | Dormancy awakening signal | Long-dormant -> sudden activity | JIL dormancy tracker | **CLEAR** | sha256:04do...w4w |
| **WIE-05** | Dust attack detection | Micro-tx flood pattern | JIL dust detector | **CLEAR** | sha256:05du...w5w |
| **WIE-06** | Fresh-wallet-with-instant-activity | Activity within 1h of creation | JIL creation telemetry | **CLEAR** | sha256:06fr...w6w |
| **WIE-07** | Bulk wallet creation signal | Sequential wallet creation cluster | JIL creation graph | **CLEAR** | sha256:07bu...w7w |
| **WIE-08** | Contamination 2-hop weighted | Graph traversal, decay-weighted exposure scoring | JIL L1 + Chainalysis | **0.02% (CLEAR)** | sha256:08co...w8c |
| **WIE-09** | Direct darknet exposure | 0-hop match to known darknet wallets | JIL known-bad registry | **CLEAR** | sha256:09di...w9c |
| **WIE-10** | Direct ransomware operator exposure | 0-hop match to ransomware wallets | JIL ransomware intel (Conti/LockBit/BlackCat/Cl0p) | **CLEAR** | sha256:10di...w0c |
| **WIE-11** | Mixer/tumbler exposure | Exposure to Tornado Cash, Blender.io, ChipMixer, Sinbad | JIL mixer registry | **CLEAR** | sha256:11mi...w1c |
| **WIE-12** | Exchange-hack cluster exposure | Mt. Gox, Bitfinex, FTX, KuCoin hack wallets | JIL hack attribution | **CLEAR** | sha256:12ex...w2c |
| **WIE-13** | Known-bad cluster exposure (full) | 0/1/2/3-hop lookup against all known-bad | JIL known-bad registry | **CLEAR** | sha256:13kn...w3c |
| **WIE-14** | State-actor cluster exposure | Lazarus Group, APT38, Russian ransomware | JIL state-actor attribution | **CLEAR** | sha256:14st...w4c |
| **WIE-15** | Transaction cadence anomaly | Inter-arrival time distribution | JIL L1 cadence analyzer | **CLEAR** | sha256:15tr...w5v |
| **WIE-16** | Amount distribution | Distribution vs 90d self-baseline | JIL amount analyzer | **CLEAR** | sha256:16am...w6v |

| CHECK ID | TEST NAME | METHOD | SOURCE | RESULT | EVIDENCE HASH |
|---|---|---|---|---|---|
| | outlier | | | | |
| **WIE-17** | Bot activity signature | Automated tx signing pattern | JIL bot detector | **CLEAR** | sha256:17bo...w7v |
| **WIE-18** | Burst-and-drain pattern | High inbound then full drain | JIL burst detector | **CLEAR** | sha256:18bu...w8v |
| **WIE-19** | Round-amount trading | Round-number frequency outlier | JIL amount analyzer | **CLEAR** | sha256:19ro...w9v |
| **WIE-20** | Fragmentation pattern | Tx split into sub-threshold batches | JIL fragmentation detector | **CLEAR** | sha256:20fr...w0v |
| **WIE-21** | Cross-chain arbitrage signature | Arbitrage-like paired tx across chains | JIL cross-chain detector | **CLEAR** | sha256:21cr...w1v |
| **WIE-22** | Protocol whitelist match | Interacted protocols in whitelist | JIL DeFi whitelist | **94/100 (HIGH TRUST)** | sha256:22pr...w2d |
| **WIE-23** | LP quality score | Uniswap / Balancer pool quality | JIL DeFi attestation ledger | **HIGH** | sha256:23lp...w3d |
| **WIE-24** | Rug-pull heuristic | Known rug-pull cluster exposure | JIL rug-pull registry | **CLEAR** | sha256:24ru...w4d |
| **WIE-25** | Yield-farming exposure | Yield-protocol interaction + risk tier | JIL yield-farm classifier | **LOW** | sha256:25yi...w5d |
| **WIE-26** | Flash-loan anomaly | Flash-loan pattern in history | JIL flash-loan detector | **CLEAR** | sha256:26fl...w6d |
| **WIE-27** | Bridge-exploit exposure | Known bridge-exploit interaction | JIL bridge-exploit registry | **CLEAR** | sha256:27br...w7d |
| **WIE-28** | Governance manipulation signal | Flash-loan governance attack pattern | JIL governance-attack detector | **CLEAR** | sha256:28go...w8d |
| **WIE-29** | Cross-wallet clustering | JIL attribution engine (BTC/EVM/SOL/TRX) | JIL attribution engines | **No discrepancy** | sha256:29cr...w9h |
| **WIE-30** | Change-address heuristic (BTC) | Multi-input + change detection | JIL attribution-btc | **CLEAR** | sha256:30ch...w0h |
| **WIE-31** | Common-ownership heuristic | Co-spending patterns across wallets | JIL attribution-btc/evm | **CLEAR** | sha256:31co...w1h |
| **WIE-32** | Bridge-correlation clustering | Cross-chain bridge traffic as identity | JIL attribution-bridges | **CLEAR** | sha256:32br...w2h |
| **WIE-33** | CEX-withdrawal correlation | CEX-withdrawal timing + amount match | JIL CEX attribution | **CLEAR** | sha256:33ce...w3h |
| **WIE-34** | Off-chain-linked wallet | Corporate entity + wallet linkage via OpenCorporates | OpenCorporates + JIL entity graph | **CLEAR** | sha256:34of...w4h |

| CHECK ID | TEST NAME | METHOD | SOURCE | RESULT | EVIDENCE HASH |
|---|---|---|---|---|---|
| **WIE-35** | Real-estate linked wallet | Property-purchase blockchain linkage | ATTOM Property + JIL entity graph | **CLEAR** | sha256:35re...w5h |
| **WIE-36** | Jurisdictional fit (corridor) | Counterparty jurisdiction vs origin corridor | GLEIF + OpenCorporates | **PASS (US-SG corridor compliant)** | sha256:36ju...w6r |
| **WIE-37** | Sanctions-list proximity | Distance to any sanctioned wallet in graph | OFAC + EU + UK SDN + JIL L1 | **> 4 hops (CLEAR)** | sha256:37sa...w7r |
| **WIE-38** | PEP overlap (counterparty UBO) | UBO graph overlap with PEP list | OpenSanctions PEP | **CLEAR** | sha256:38pe...w8r |
| **WIE-39** | Adverse media flag | Counterparty name in adverse-media feed | OpenSanctions media + Dow Jones | **CLEAR** | sha256:39ad...w9r |
| **WIE-40** | Taint-free proof | Cumulative contamination score under 1% | JIL taint calculator | **0.02% (PASS)** | sha256:40ta...w0r |
| **WIE-41** | MiCA stablecoin eligibility | Token MiCA-registered flag | EBA MiCA registry | **PASS** | sha256:41mi...w1r |
| **WIE-42** | Travel-rule data completeness | Originator+beneficiary data fields populated | IVMS 101 validator | **PASS** | sha256:42tr...w2r |

## 3 OUT-OF-SCOPE CHECKS - NOT ENABLED (SECTION 4B)

69 OUT OF SCOPE

Listed for transparency. These checks exist in the 111-check catalog but were not enabled in this profile. Their omission is explicit, auditable, and court-defensible.

| CHECK ID | TEST NAME | STATUS |
|---|---|---|
| FWEA-01 | OFAC person match (origin) | *Out of scope - not enabled in this profile* |
| FWEA-02 | OFAC person match (counterparty) | *Out of scope - not enabled in this profile* |
| FWEA-03 | PEP screening - beneficial owners | *Out of scope - not enabled in this profile* |
| FWEA-04 | Synthetic identity detection | *Out of scope - not enabled in this profile* |
| FWEA-05 | Document deepfake detection | *Out of scope - not enabled in this profile* |
| FWEA-06 | AI voice deepfake at authorization | *Out of scope - not enabled in this profile* |
| FWEA-07 | Destination wallet SDN match | *Out of scope - not enabled in this profile* |
| FWEA-08 | Business Email Compromise (BEC) pattern | *Out of scope - not enabled in this profile* |
| FWEA-09 | Invoice fraud detection | *Out of scope - not enabled in this profile* |
| FWEA-10 | Account takeover (ATO) signals | *Out of scope - not enabled in this profile* |
| FWEA-11 | Authorized Push Payment (APP) scam | *Out of scope - not enabled in this profile* |
| FWEA-12 | Wire anomaly detection | *Out of scope - not enabled in this profile* |
| FWEA-13 | SEPA APP fraud pattern (EU) | *Out of scope - not enabled in this profile* |
| FWEA-14 | UK FPS Payment System Regulator (PSR) profile | *Out of scope - not enabled in this profile* |
| FWEA-15 | PIX fraud typology (Brazil) | *Out of scope - not enabled in this profile* |
| FWEA-16 | UPI fraud typology (India) | *Out of scope - not enabled in this profile* |
| FWEA-17 | SWIFT gpi chain substitution | *Out of scope - not enabled in this profile* |
| FWEA-18 | CIPS sanctioned-entity routing | *Out of scope - not enabled in this profile* |
| FWEA-19 | NPP PayID integrity (Australia) | *Out of scope - not enabled in this profile* |
| FWEA-20 | DPAN wallet provisioning fraud | *Out of scope - not enabled in this profile* |
| FWEA-21 | Magecart / e-skimmer merchant compromise | *Out of scope - not enabled in this profile* |
| FWEA-22 | Cryptocurrency off-ramp anomaly | *Out of scope - not enabled in this profile* |
| FWEA-23 | Check kite / float fraud | *Out of scope - not enabled in this profile* |
| FWEA-24 | Settlement instruction integrity | *Out of scope - not enabled in this profile* |
| FWEA-25 | OFAC country-level sanctions | *Out of scope - not enabled in this profile* |
| FWEA-26 | EU MiCA stablecoin classification | *Out of scope - not enabled in this profile* |
| FWEA-27 | EU DORA operational resilience | *Out of scope - not enabled in this profile* |
| FWEA-28 | UK FCA authorization status | *Out of scope - not enabled in this profile* |
| FWEA-29 | FATF International Travel Rule (>$3K) | *Out of scope - not enabled in this profile* |
| FWEA-30 | CBDC attestation (eCNY / DEUR / mBridge) | *Out of scope - not enabled in this profile* |

| CHECK ID | TEST NAME | STATUS |
|---|---|---|
| **FWEA-31** | NYDFS Part 500 applicability | *Out of scope - not enabled in this profile* |
| **FWEA-32** | SEC Reg S / Reg D (if applicable) | *Out of scope - not enabled in this profile* |
| **FWEA-33** | MAS Singapore DPT Act applicability | *Out of scope - not enabled in this profile* |
| **FWEA-34** | VARA UAE crypto licensing | *Out of scope - not enabled in this profile* |
| **FWEA-35** | State MTL jurisdiction check | *Out of scope - not enabled in this profile* |
| **FWEA-36** | Velocity anomaly (origin 48h) | *Out of scope - not enabled in this profile* |
| **FWEA-37** | Mule account scoring | *Out of scope - not enabled in this profile* |
| **FWEA-38** | Smurfing / structuring pattern | *Out of scope - not enabled in this profile* |
| **FWEA-39** | Geographic anomaly | *Out of scope - not enabled in this profile* |
| **FWEA-40** | Bust-out credit fraud pattern | *Out of scope - not enabled in this profile* |
| **FWEA-41** | Round-amount / psychological pricing flag | *Out of scope - not enabled in this profile* |
| **FWEA-42** | Night / off-hours activity | *Out of scope - not enabled in this profile* |
| **FWEA-43** | Routing change detection (<72h) | *Out of scope - not enabled in this profile* |
| **FWEA-44** | Account-number change alert | *Out of scope - not enabled in this profile* |
| **FWEA-45** | Instruction provenance attestation | *Out of scope - not enabled in this profile* |
| **FWEA-46** | IBAN integrity (MOD-97) | *Out of scope - not enabled in this profile* |
| **FWEA-47** | Correspondent chain hop anomaly | *Out of scope - not enabled in this profile* |
| **FWEA-48** | Real estate closing wire protection | *Out of scope - not enabled in this profile* |
| **FWEA-49** | Endpoint binding attestation | *Out of scope - not enabled in this profile* |
| **FWEA-50** | Duplicate claim detection | *Out of scope - not enabled in this profile* |
| **FWEA-51** | NPI provider enrollment status | *Out of scope - not enabled in this profile* |
| **FWEA-52** | Upcoding detection | *Out of scope - not enabled in this profile* |
| **FWEA-53** | Remittance mismatch | *Out of scope - not enabled in this profile* |
| **FWEA-54** | Overpayment recovery flag | *Out of scope - not enabled in this profile* |
| **FWEA-55** | Fraud ring graph analysis | *Out of scope - not enabled in this profile* |
| **FWEA-56** | Typology library pattern match | *Out of scope - not enabled in this profile* |
| **FWEA-57** | Cross-rail correlation | *Out of scope - not enabled in this profile* |
| **FWEA-58** | FaaS (Fraud-as-a-Service) infrastructure | *Out of scope - not enabled in this profile* |
| **FWEA-59** | FATF typology pattern match | *Out of scope - not enabled in this profile* |
| **FWEA-60** | Egmont FIU intelligence overlay | *Out of scope - not enabled in this profile* |
| **FWEA-61** | BIS CPMI payment system risk | *Out of scope - not enabled in this profile* |
| **FWEA-62** | Cross-border velocity multi-jurisdiction | *Out of scope - not enabled in this profile* |
| **FWEA-63** | Sanctioned-jurisdiction hub routing | *Out of scope - not enabled in this profile* |
| **FWEA-64** | TBML with World Bank commodity prices | *Out of scope - not enabled in this profile* |
| **FWEA-65** | Pig butchering / romance-investment scam | *Out of scope - not enabled in this profile* |

| CHECK ID | TEST NAME | STATUS |
|---|---|---|
| **FWEA-66** | FaaS C2 infrastructure attribution | *Out of scope - not enabled in this profile* |
| **FWEA-67** | ZKP post-settlement attestation | *Out of scope - not enabled in this profile* |
| **FWEA-68** | Adversarial ML drift detection | *Out of scope - not enabled in this profile* |
| **FWEA-69** | HNDL quantum-safe TLS verification | *Out of scope - not enabled in this profile* |

## 5 FINAL VERDICT

ATTESTED DISPOSITION

# RISK SCORE 23/100

Confidence: 97.1% | LOW RISK - Withdrawal approved. Re-evaluation triggered if score exceeds 60.

REASONING SUMMARY

- Wallet age 847 days (LOW RISK, WIE-01)
- Counterparty contamination (2-hop weighted): 0.02% (WIE-08, CLEAR)
- No direct darknet / ransomware / mixer / state-actor exposure (WIE-09 through WIE-14, CLEAR)
- Velocity patterns within 90-day baseline (WIE-15, CLEAR)
- DeFi trust score 94/100 (WIE-22, HIGH TRUST)
- Cross-wallet clustering: no discrepancy with declared holdings (WIE-29, CLEAR)
- Regulatory alignment: US-SG corridor compliant (WIE-36, PASS)
- Cumulative taint score: 0.02% (WIE-40, under 1% threshold)

## 6 CRYPTOGRAPHIC SEAL AND ANCHOR

**Issuer**
`JIL Sovereign Technologies, Inc. (DE)`

**Signing Algorithm**
`Ed25519 + Dilithium-III (classical + post-quantum hybrid)`

**Issuer Signature**
`c3d4e5f67890a1b2abcdef0123456789fedcba9876543210abcdef0123456789`

**Validator Quorum**
`14 of 20 across 10 jurisdictions (70% threshold exceeded)`

**JIL L1 Anchor**
`tx-hash: 0xcd34...678e`

**Merkle Root**
`Rolled up from Section 4A per-check evidence hashes`

Verify at
**jilsovereign.com/verify/JIL-VR-WI-2026-04-19-D5C**

## 7 CHAIN OF CUSTODY TIMELINE

| | | |
|---|---|---|
| **15:03:51.000 UTC** | Exchange POST /api/wie/verdict received | `req-hash: 4d5e6f7a8b9c...` |
| **15:03:51.014 UTC** | Test profile WIE-STANDARD-v4.0 loaded | `profile-hash: 0d1e2f3a4b5c...` |
| **15:03:51.023 UTC** | 42 WIE signals dispatched | `dispatch-hash: 6d7e8f9a0b1c...` |
| **15:03:51.161 UTC** | All 42 signals returned. Risk score aggregated. | `signals-hash: 2d3e4f5a6b7c...` |
| **15:03:51.169 UTC** | Verdict sealed (Ed25519 + Dilithium-III) | `verdict-hash: 8d9e0f1a2b3c...` |
| **15:03:51.175 UTC** | Validator quorum (14/20) signed | `quorum-hash: 4d5e6f7a8b9c...` |
| **15:03:51.182 UTC** | Anchored to JIL L1 block #892,448 | `tx-hash: 0xcd34...678e` |
| **15:03:51.185 UTC** | Record written to exchange SDV | `sdv-object: verdicts/wallet-intel/2026/04/19/...` |
| **15:03:51.187 UTC** | Retrieval-index commit | `index-id: VR-INDEX-1776657831187` |

Total latency: **187 ms** - within the 200ms WIE SLA.

> **Tamper Evidence.** Any modification to this record - including whitespace, font, or formatting changes after issuance - invalidates the seal. Independent verification does not require JIL Sovereign's cooperation and can be performed by any party that can compute a SHA-256 hash, verify an Ed25519 signature, and query the JIL L1 public ledger for the anchor transaction. The verification procedure is published at **jilsovereign.com/verify** and is open-source.

## 8 AUTHORIZED EVIDENTIARY USES

- Federal court admission under **FRE 702** (expert testimony) and **901** (authentication) - cryptographic anchor authenticates without requiring JIL as fact witness.
- Regulatory submission to OFAC, FinCEN, SEC, and state attorneys general.
- Custodian compliance evidence for SOC 2 Type II, ISO 27001, NYDFS Part 500, HITRUST CSF audits.
- Internal audit trail under BSA 5-year recordkeeping (JIL retention exceeds at 15+ years).
- Due diligence evidence for correspondent banking, MSB registration, VASP Travel Rule.

**JIL Sovereign Technologies, Inc.** - Delaware C-Corporation - Dallas, Texas
Patent portfolio: 48 issued, 11 in flight. This record is *not* financial advice. It is an attested computational result. It is a fact, not an opinion.
Questions: **verify@jilsovereign.com** - Response SLA: 24 hours.