JIL Sovereign Technologies, Inc.
CRYPTOGRAPHIC VERDICT AUTHORITY - PILLAR 3

REPORT IDENTIFIER
JIL-VR-AI-2026-04-19-C7D6E5F4
Issued: 2026-04-19 11:02:17 UTC
Completed: 2026-04-19 11:08:44.218 UTC

PILLAR 3 OF 5 - ASSET INTELLIGENCE DOSSIER

Cryptographic Verdict Record

Court-Admissible - Independently Verifiable - Tamper-Evident

SAMPLE - FICTITIOUS SUBJECT DATA

0 IDENTIFIERS, RETRIEVAL, AND RETENTION

Report ID (this document)	`JIL-VR-AI-2026-04-19-C7D6E5F4`
Attestation ID	`ATT-892432-0000001584`
Vendor ID (requester)	`VND-TRUSTEE-0089 (Chapter 11 Trustee, Eastern District of New York, onboarded 2026-02-14)`
Profile ID	`PRF-ASSET-INVEST-JURISDICTION-STANDARD-v2.1`
Date Completed	2026-04-19 11:08:44.218 UTC (epoch `1776639524.218`)
Storage Location (vendor-controlled)	Vendor SDV endpoint `sdv://VND-TRUSTEE-0089.us-east.jil-sdv/`, object key `verdicts/asset-intel/2026/04/19/JIL-VR-AI-2026-04-19-C7D6E5F4.pdf.sealed`. AES-256-GCM encrypted, vendor-held key.
Content Hash (SHA-256)	`b2c3d4e5f67890a1fedcba98765432100123456789abcdef0123456789abcdef`
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	Asset Intelligence Dossier (Pillar 3) - JIL Agent + Fabric + Reconcile
Requesting Party	Redacted Chapter 11 Trustee, Case `26-47215-xxx`, EDNY Bankruptcy Court
Subject of Investigation	Redacted Debtor Entity and Principals (collectively, "Subject"), investigation scope bounded by trustee letter 2026-04-12
Claimed Assets (Schedule A/B)	$2,100,000 total (real property + securities + business interests)
Discovered Assets	$7,432,500 total (6 on-chain wallets + 3 off-chain corporate entities + 2 undisclosed real properties + 1 undisclosed trust)
Reconciled Discrepancy	$5,332,500 (on-chain $3.1M + off-chain $2.2M)
Investigation Lead Analyst	Redacted Senior Forensic Accountant (CFE, CAMS), Analyst-ID `an:9c1a:3b4e:5f6d`
Agent Trace	LangGraph deterministic mode, 127 tool invocations, all cryptographically logged

2 TEST PROFILE APPLIED

Profile Name	`ASSET-INVEST-JURISDICTION-STANDARD-v2.1`
Profile Description	Standard forensic asset investigation. Entity resolution + off-chain fusion + WIE + typology.
Total Catalog Size	111 checks (69 FWEA + 42 WIE)
Approved for this Profile	**61 of 111** checks enabled
Out of Scope (not approved)	50 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)

61 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
FWEA-01	OFAC person match (origin)	Exact + fuzzy (Levenshtein <=2, phonetic Soundex)	OFAC SDN + CSL	**CLEAR**	`sha256:01of...f1i`
FWEA-02	OFAC person match (counterparty)	Exact + fuzzy + transliteration	OFAC SDN + CSL + EU + UK	**CLEAR**	`sha256:02of...f2i`
FWEA-03	PEP screening - beneficial owners	UBO graph traversal to depth 3	OpenSanctions PEP list	**CLEAR**	`sha256:03pe...f3i`
FWEA-04	Synthetic identity detection	Document cross-reference + velocity modeling	GLEIF + OpenCorporates + telco records	**CLEAR**	`sha256:04sy...f4i`
FWEA-05	Document deepfake detection	Signature + metadata + font analysis	JIL document integrity ML	**CLEAR**	`sha256:05do...f5i`
FWEA-06	AI voice deepfake at authorization	Spectral + prosodic + behavioral analysis	JIL voice auth ML	**CLEAR**	`sha256:06ai...f6i`
FWEA-07	Destination wallet SDN match	O(1) hash-table lookup (<1ms)	OFAC SDN + CSL + UK OFSI	**CLEAR**	`sha256:07de...f7i`
FWEA-55	Fraud ring graph analysis	Community detection on entity graph	JIL fraud-ring detector	**CLEAR**	`sha256:55fr...f5m`
FWEA-56	Typology library pattern match	Published typology overlay (pig-butchering, APP, etc)	JIL typology library v3	**CLEAR**	`sha256:56ty...f6m`
FWEA-57	Cross-rail correlation	Same entity on multiple rails	JIL entity resolution	**CLEAR**	`sha256:57cr...f7m`
FWEA-58	FaaS (Fraud-as-a-Service) infrastructure	Known FaaS C2 + tooling signature	JIL FaaS intel	**CLEAR**	`sha256:58fa...f8m`
FWEA-59	FATF typology pattern match	Graph-motif match across 30d window	JIL L1 + Chainalysis clusters	**CLEAR**	`sha256:59fa...f9c`
FWEA-60	Egmont FIU intelligence overlay	FIU-flagged entity check	Egmont Group secure channel	**CLEAR**	`sha256:60eg...f0c`
FWEA-61	BIS CPMI payment system risk	Payment corridor risk score	BIS CPMI annual report data	**LOW**	`sha256:61bi...f1c`
FWEA-62	Cross-border velocity multi-jurisdiction	Velocity across 3+ jurisdictions 7d	JIL cross-border detector	**CLEAR**	`sha256:62cr...f2c`

CHECK ID	TEST NAME	METHOD	SOURCE	RESULT	EVIDENCE HASH
FWEA-63	Sanctioned-jurisdiction hub routing	Proximity to sanctioned corridor	OFAC country list + corridor graph	**CLEAR**	sha256:63sa...f3c
FWEA-64	TBML with World Bank commodity prices	Invoice-price variance vs market	World Bank commodity index + WCO	**CLEAR**	sha256:64tb...f4c
FWEA-65	Pig butchering / romance-investment scam	Behavior + destination + dialog ML	JIL pig-butcher registry + NIST	**CLEAR**	sha256:65pi...f5e
FWEA-66	FaaS C2 infrastructure attribution	Infrastructure overlap with known FaaS	JIL FaaS infra graph	**CLEAR**	sha256:66fa...f6e
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

CHECK ID	TEST NAME	METHOD	SOURCE	RESULT	EVIDENCE HASH
WIE-15	Transaction cadence anomaly	Inter-arrival time distribution	JIL L1 cadence analyzer	**CLEAR**	sha256:15tr...w5v
WIE-16	Amount distribution outlier	Distribution vs 90d self-baseline	JIL amount analyzer	**CLEAR**	sha256:16am...w6v
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 + JIL entity graph	**CLEAR**	sha256:34of...w4h

CHECK ID	TEST NAME	METHOD	SOURCE	RESULT	EVIDENCE HASH
		OpenCorporates			
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)

50 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-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*
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*

CHECK ID	TEST NAME	STATUS
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-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

DISCREPANCY SEALED

Confidence: 94.8% | $5,332,500 in undisclosed assets identified with full evidentiary chain

REASONING SUMMARY

- JIL Agent executed 127 investigation tool calls across JIL Fabric (on-chain + off-chain)
- 6 wallets clustered to Subject via WIE-29 cross-wallet clustering and WIE-33 CEX-withdrawal correlation
- 3 corporate entities linked via WIE-34 off-chain entity graph (OpenCorporates + UBO depth-3)
- 2 real properties linked via WIE-35 (ATTOM Property + JIL entity graph)
- JIL Reconcile parsed Schedule A/B and emitted sealed verdicts on every omission (12 items, 5 material)
- All exhibits independently Ed25519-signed; aggregate Merkle root anchored to JIL L1 block #892,420
- Dossier structured for FRE 702 / 901 admission; trustee letter-grade (expert-witness-ready)

6 CRYPTOGRAPHIC SEAL AND ANCHOR

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

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

Issuer Signature
`b2c3d4e5f67890a1fedcba9876543210012345678 9abcdef0123456789abcdef`

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

JIL L1 Anchor
`tx-hash: 0xab23...567d`

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

Verify at
jilsovereign.com/verify/JIL-VR-AI-2026-04-19-C7D

7 CHAIN OF CUSTODY TIMELINE

11:02:17.044 UTC	Trustee POST /investigate received; scope bounded	`req-hash: 3c4d5e6f7a8b...`
11:02:19.882 UTC	Test profile ASSET-INVEST-JURISDICTION-STANDARD-v2.1 loaded	`profile-hash: 9c0d1e2f3a4b...`
11:02:24.113 UTC	JIL Agent plan generated: 127 tool invocations across Fabric	`plan-hash: 5c6d7e8f9a0b...`
11:06:48.709 UTC	All tool invocations complete; entity graph materialized	`graph-hash: 1c2d3e4f5a6b...`
11:07:02.553 UTC	JIL Reconcile compared claimed vs discovered; 12 discrepancies flagged	`reconcile-hash: 7c8d9e0f1a2b...`
11:08:11.241 UTC	61 approved checks run against graph; 4 signals flagged (velocity + UBO)	`checks-hash: 3c4d5e6f7a8b...`
11:08:28.008 UTC	12 individual discrepancy verdicts sealed	`disc-root: 9c0d1e2f3a4b...`
11:08:41.119 UTC	Validator quorum (14/20) signed	`quorum-hash: 5c6d7e8f9a0b...`
11:08:43.617 UTC	Dossier anchored to JIL L1 block #892,420	`tx-hash: 0xab23...567d`
11:08:44.218 UTC	Court-ready dossier delivered to trustee SDV	`sdv-object: verdicts/asset-intel/2026/04/19/...`
11:08:44.402 UTC	Retrieval-index commit; 15-year retention class	`index-id: VR-INDEX-1776639524218`

Total investigation latency: **6 minutes 27 seconds** - including 127 Agent tool invocations and full Fabric graph materialization.

> **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.