ARCHITECTURE & ECOSYSTEM · V1.0 · MAY 2026

Trust, *Restored.*

A bi-directional payment integrity network. Built on a sovereign Layer 1 blockchain. Engineered to put admissible proof back into finance.

JIL Sovereign Technologies, Inc.

JILSOVEREIGN.COM · AN ARCHITECTURE REFERENCE FOR THE INSTITUTIONAL READER

FOUNDATION
CourtChain L1

VALIDATORS
5 Jurisdictional Vaults

VERTICALS
Nine Live

STATUS
Production

Foreword

Payment fraud has crossed a trillion dollars a year. The systems built to stop it cannot scale. The systems built to prove it cannot travel. We built JIL because finance needs a different foundation, one designed from the start to produce admissible truth at the speed of a wire transfer.

This document is the architecture reference for that foundation. It is written for the institutional reader: the chief information officer choosing where payment integrity will

live, the general counsel asking whether a finding can stand up in court, the inspector general planning recovery action, the foundation president signing off on a grantee. It is also written for the engineer, the auditor, and the regulator who will look closely at how the parts fit together.

JIL is not a tool that bolts onto an existing fraud system. JIL is a network. It runs on a purpose-built Layer 1 blockchain we call CourtChain, distributed across five sovereign jurisdictions. On top of that foundation sits a Verdict Engine that runs 175 attestation checks across 15 categories, deployed across nine verticals, in sub-second time. On top of that engine, six product lines serve every major surface where money moves. And on top of those products, a set of customer-facing applications connects institutions, foundations, treasuries, and consumers to the same trusted record.

What follows describes each of those layers, what they do, why they exist, how they fit together, and how you adopt them. We have tried to make it exhaustive without being exhausting.

How to read this paper

Read sequentially for the full thesis. Or jump to the section that matches your role.

PART I

Why this exists.

Three structural problems define payment fraud at scale. JIL was built to close all three at once.

Money moves faster than oversight. The global payment system processes hundreds of billions of dollars in transactions every day across rails that were never designed to verify intent, identity, or eligibility at speed. Fraud was supposed to be the exception. Today, by every reputable measure, it is a structural cost. The Federal Trade Commission tracks consumer reports topping ten billion dollars in losses annually. The Association of Certified Fraud Examiners estimates organizations lose roughly five percent of revenue to occupational fraud. Health care payment integrity offices estimate hundreds of billions a year in improper payments at the federal level alone. Cross-border, the picture compounds. Sanctions evasion, beneficial-ownership shielding, and stablecoin laundering turn what used to be jurisdictional problems into networked ones.

The numbers obscure a deeper problem. Payment systems are losing the ability to produce *proof.* When a claim is later disputed, when a wire is later reversed, when a grantee is later investigated, the institution that paid the money often cannot show, with cryptographic precision, what it knew and when it knew it. Audit trails are partial. Reasoning is implicit. Evidence is not portable. The Federal Rules of Evidence still require, under Rule 902(14), that digital records be self-authenticating before they walk into court. Most enterprise fraud platforms produce alerts. They do not produce records that meet that bar.

Three failures, one architecture

The structural failures cluster into three categories, and JIL addresses each one with a specific architectural choice.

FAILURE 01

Settlement is final.

Most fraud is detected after the money has moved. Recovery is expensive, slow, and often impossible across jurisdictions. The economics of recovery are punishing once funds clear. JIL closes this gap with **Pre-Settlement**, blocking improper payments before they finalize.

FAILURE 02

Each payer fights alone.

Bad actors move freely between MCOs, banks, federal agencies, and borders. No single payer sees the whole pattern. The criminals do. JIL closes this gap with the **Bad Actor Registry**, a cross-customer knowledge graph that compounds with every transaction observed.

FAILURE 03

Evidence does not travel.

Detection systems produce alerts, not court-admissible records. By the time a case is built,

the trail is cold. JIL closes this gap with **CREB**, the Court Ready Evidence Model, anchored to **CourtChain**, a sovereign Layer 1 ledger.

What makes JIL different is not that we identified these three problems. Anyone in payment integrity can name them. What makes JIL different is that we built one platform that solves all three on a single foundation, in a single mathematical model, deployable in any major cloud the customer prefers. The work took two and a half years and roughly 1.5 million lines of code. The result is in production today.

THESIS IN ONE SENTENCE

JIL stops bad payments before they settle, proves good payments after they do, and anchors both into a chain that no single party, including JIL, can rewrite.

PART II

The L1 thesis.

Why a payment integrity network needs its own Layer 1 blockchain, and why a database, an L2, or a permissioned ledger does not satisfy the requirement.

JIL begins with an unusual claim for a payment integrity company. We argue that the foundation of the platform must be a sovereign Layer 1 blockchain, not a database, not a Layer 2 rollup, not a permissioned ledger run by JIL or by a consortium. The choice is consequential. It shapes every layer above it. It is also the single most common point of skepticism we encounter in early conversations with chief information officers, who tend to reach reflexively for the database answer. The skepticism is fair. The answer is specific.

What a regular database cannot do

A relational database has one administrator who can edit any record. A modern data warehouse has perhaps a dozen administrators with different scopes, but the property is the same: somewhere, at some level, a privileged user can change what was written. For most enterprise workloads, this is a feature. For evidence, it is fatal. Federal Rule of Evidence 902(14), the rule that governs self-authenticating digital evidence, requires a process that demonstrably cannot be tampered with by any single party. A database run by JIL fails the test trivially. A database run by the customer fails it because the customer is a party to the dispute. A database run by a third-party auditor fails it because the auditor is also a single point of failure.

This is not theoretical. In any meaningful payment dispute, opposing counsel will ask the same question: who could have changed this record between the time it was written and the time it was produced in discovery? If the answer is anyone, the record is impeachable. If the answer is no one, the record is not.

What a permissioned chain cannot do

A permissioned blockchain run by a consortium improves the picture only if the consortium is genuinely independent. In practice, consortia consolidate. Members are subject to common pressures from regulators, courts, and acquirers. A subpoena to one validator can extend to all. Worse, the most useful payment integrity networks span jurisdictions that do not consistently honor each other's compulsion. A consortium incorporated in a single country cannot offer the neutrality that cross-border evidence demands.

What an L2 cannot do

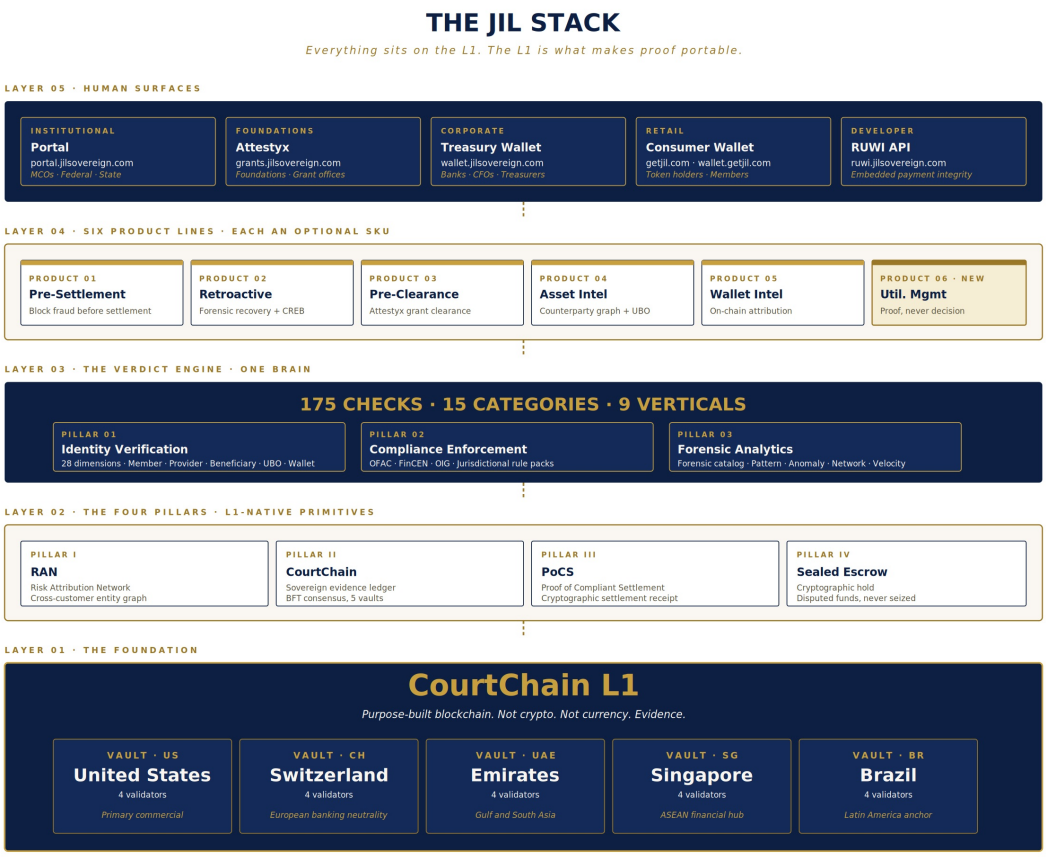
Layer 2 networks inherit security from a Layer 1, but they also inherit policy from the Layer 1. An L2 settling onto a public chain is bound by that chain's social and regulatory pressure. For most blockchain applications, that inheritance is acceptable. For an evidence chain that may be queried by federal investigators in matters involving the underlying L1's largest stakeholders, the inheritance is a conflict.

Why we built our own L1

JIL operates CourtChain, a purpose-built Layer 1 ledger. It is in production today. It is not a fork of an existing chain. It is not a sidechain. It is not anchored into Bitcoin or Ethereum. It is its own consensus, its own validator set, and its own jurisdictional distribution, designed for one job: producing self-authenticating digital records of payment integrity decisions that no single party, including JIL, can rewrite.

The figure on the next page shows how everything else in the JIL platform sits on top of CourtChain. Every product line, every customer surface, every verdict, every CREB roots into the same ledger. That is the architecture. It is also the moat.

FIGURE 1 · THE JIL STACK



Five layers, from foundation to surface. Every layer above the L1 is replaceable. The L1 itself is what makes proof portable across products, customers, and jurisdictions.

PART III

CourtChain L1: the foundation.

Twenty validators distributed across five jurisdictions. Byzantine Fault Tolerant consensus. Sub-second finality. Post-quantum cryptography. Hashes only on the wire.

CourtChain is JIL's purpose-built Layer 1 blockchain. It anchors every verdict, every CREB, and every settlement event the platform produces. It is not a marketplace. It does not host smart contracts written by third parties. It does not have a public mempool. It runs one job, and it runs it with the integrity properties a courthouse demands.

The validator set

CourtChain's consensus layer is operated by twenty validators, with another twenty on standby for resilience. Validators are distributed across five jurisdictional vaults: the United States, Switzerland, the United Arab Emirates, Singapore, and Brazil. Each vault is

operated under different legal authority and different physical custody. Tampering with the chain would require simultaneously compromising validators in five different countries. That bar is essentially uncrossable, both technically and politically. Beyond the five anchor vaults, the design supports operational validators in thirteen or more additional jurisdictions, allowing customers in regulated regions to participate in the network from inside their own legal framework.

Consensus

CourtChain runs Byzantine Fault Tolerant consensus, with finality requiring a two-thirds plus one supermajority of validators to sign any block. There is no probabilistic finality, no orphan blocks, no chain reorganizations. When the network confirms a block, the block is final. Performance is sub-second on a modern hardware fleet. Throughput exceeds the requirements of every customer use case we have tested.

Cryptography

Every signature on CourtChain is a hybrid of Ed25519 and Dilithium-III. Block hashes use ML-DSA-65, a NIST-standardized post-quantum cryptographic primitive. The hybrid construction means CourtChain remains secure against both classical and quantum adversaries. A sufficiently capable quantum computer breaking Ed25519 in the future would still face the post-quantum lattice in Dilithium-III. The combined posture is what federal customers and long-horizon institutional customers need to trust the chain with evidence that may be litigated a decade from now.

What flows on the wire

CourtChain stores hashes. Not claim contents. Not personal health information. Not personally identifying information. Not transaction amounts in plaintext. Validators see and sign cryptographic commitments to evidence packages that live, in their full form, inside the customer's data plane. This is not an oversight. It is a deliberate design property. The chain is portable, queryable, and verifiable by any regulator, but it carries no payload that a regulator could compel JIL to disclose. The customer holds the original. The chain holds the proof that the original existed at a specific point in time, said specifically what it said, and produced specifically what it produced.

> **PROPERTY**
>
> *CourtChain is the courthouse. JIL files documents at the courthouse. The customer keeps stamped receipts back at the office. Master records sit at five courthouses across five jurisdictions. The customer cannot, and need not, run the courthouse.*

PART IV

The four pillars.

RAN, CourtChain, PoCS, Sealed Escrow. Four operational

primitives. Every product on the platform composes them.

The platform's surface area is large. The customer-visible products are six. The internal services number in the hundreds. Behind all of it sit four operational primitives that anchor the architecture. We call them the four pillars. Every product on the JIL platform is some composition of them. New products will be too.

Pillar I: RAN, the Risk Attribution Network

RAN is the shared knowledge graph that links entities, wallets, identities, networks, and patterns across all customers and jurisdictions. It is the substrate of the Bad Actor Registry, but it is more than the registry. RAN is the layer that resolves an inbound claim to a real-world counterparty, a real-world beneficial owner, a real-world wallet attribution, and a real-world risk profile. Every product line queries RAN. RAN itself lives on the JIL Sovereign Network and is queried by customer services through controlled APIs. It does not replicate into customer infrastructure.

Pillar II: CourtChain, the sovereign evidence ledger

CourtChain is the Layer 1 ledger described in Part III. Architecturally, it is the trust root. Every verdict and CREB the Verdict Engine produces is hashed and anchored to CourtChain. Once anchored, the record is immutable. The customer can independently verify any block, any signature, any anchor proof, against the public block headers and validator signatures that CourtChain publishes.

Pillar III: PoCS, Proof of Compliant Settlement

PoCS is the cryptographic receipt that a payment cleared every required check. It is generated when the Verdict Engine returns Allow on a transaction. The PoCS receipt commits to the verdict, the rule pack version, the timestamp, the customer identity, the source data fingerprints, and the validator block height. A customer holding a PoCS receipt can prove, in the language a regulator or court will accept, that a specific payment was screened by JIL, passed every applicable check, and was anchored to CourtChain at a specific moment in time. PoCS is what makes "we cleared this" portable.

Pillar IV: Sealed Escrow, the cryptographic hold

When the Verdict Engine returns Block on a transaction, the customer's settlement workflow needs somewhere to put the disputed funds. Sealed Escrow is that place. Funds are held under a cryptographic seal, with release conditions encoded as policy. The customer's money never leaves the customer's account or its banking partners' control. The bad actor never gets paid. The dispute resolves through the customer's existing legal and operational processes. Sealed Escrow does not custody money. It custodies the cryptographic key that authorizes release, and only the customer's authorized roles can compose the conditions for that release.

The Verdict Engine.

One brain. 175 attestation checks across 15 categories, deployed across nine verticals. Three pillars of analysis. Three possible verdicts. Sub-second on every transaction.

The Verdict Engine is JIL's reasoning core. Every product line, regardless of its surface or its customer audience, terminates in a call to the same engine. This is the architectural decision that lets JIL maintain consistency across an MCO use case, a federal grants use case, a corporate treasury use case, and a retail wallet use case. The behavior is the same brain in different deployments.

The three pillars of analysis

PILLAR 01

Identity Verification

Twenty-eight identity dimensions across member, provider, beneficiary, counterparty, wallet, and network. Cross-product entity resolution. The engine treats identity as a graph, not a row.

PILLAR 02

Compliance Enforcement

OFAC, FinCEN, OIG, jurisdictional rule packs, and federal program eligibility. Sanctions corridors are traversed, not just matched. Policy is enforced as code, not as PDF.

PILLAR 03

Forensic Analytics

The forensic catalog covers pattern, behavior, network, anomaly, outlier, velocity, and cross-claim collusion. The forensic catalog is what catches the schemes that the rule layer does not name.

The three verdicts

For every transaction the engine evaluates, the output is one of three verdicts.

1. **Allow.** Cleared. A PoCS receipt is generated. The hash anchors to CourtChain. The customer can prove the payment was screened. The transaction proceeds without human intervention.
2. **Review.** Held for human eyes. An evidence bundle is generated and routed to the appropriate reviewer, whether that is the plan's medical team, a compliance officer, or a foundation's program officer. The decision the human makes is logged, anchored, and incorporated into the engine's training signal.
3. **Block.** Stopped at the gate. Funds, if any, are held in Sealed Escrow. A CREB package is built, sealed, and anchored. Findings are admissible, not merely indicative.

The three verdicts are designed to map cleanly onto the operational realities of every customer audience. An MCO does not want the engine making medical necessity decisions. A foundation does not want the engine deciding which grantee gets funded. A

treasury does not want the engine cancelling payments unilaterally. The engine surfaces the answer with the proof. The customer's authorized decision-makers act on it.

PART VI

CREB: court-ready evidence.

The artifact a federal IG, a state attorney general, opposing counsel, or a foundation board actually wants.

CREB is JIL's flagship output. It stands for **Court Ready Evidence Model**, and it is a JIL trademark. Every Review and Block verdict produces one. Every Allow verdict produces a related artifact, the PoCS receipt, that occupies the same evidentiary tier. CREB is what we mean when we say JIL is a "detection and proof" company. The detection is the verdict. The proof is the CREB.

A CREB package is engineered to satisfy Federal Rule of Evidence 902(14). That rule, adopted in 2017, allows digital records produced by a process shown to be trustworthy to be admitted into evidence without a human witness laying foundation. The rule's introduction was a response to the explosion of digital evidence in modern litigation. It is the legal mechanism by which a CREB walks into a courtroom on its own.

What every CREB contains

COMPONENT	CONTENTS
Verdict and reasoning trace	Which checks fired, which thresholds were crossed, what evidence supported each decision. The reasoning is traceable, not opaque.
Cryptographic provenance	Signed by the Verdict Engine. Timestamped. Hash anchored to CourtChain at the moment of generation. The signature chain extends from the rule pack version to the validator block height.
Source references	Pointers to the underlying claim, member record, provider profile, or counterparty graph snapshot, without exposing PHI or PII on the wire. Verifiable on demand inside the customer's data plane.
Validator attestations	Two-thirds plus one supermajority signatures from jurisdictionally independent validators on the anchor block.
Rule pack version	Exact version of the rule pack in force at evaluation time. Reproducibility of any CREB requires no operational state beyond the chain itself.
Counterparty graph snapshot	The portion of the Bad Actor Registry that informed the verdict, hashed and committed at evaluation time. The customer can demonstrate not only that JIL flagged the entity, but precisely what JIL knew about that entity at that moment.

FEDERAL RULE OF EVIDENCE 902(14)

Records generated by a process shown to be trustworthy are admissible without a human witness to lay foundation. CREB is engineered to be that record. The chain is the trustworthy process.

PART VII

The Six *Product Lines.*

One Verdict Engine. Six SKUs. Each one optional. Each one anchored to CourtChain.

7.1 Pre-Settlement

Block fraud and improper payments before they finalize.

Pre-Settlement is JIL's flagship real-time product. It runs the full Verdict Engine against every inbound claim, prior authorization request, or wire in real time. Sub-eight-hundred-millisecond verdicts mean the customer's payment rails do not slow down. Bad payments are stopped at the gate. Good payments receive a Proof of Compliant Settlement receipt. The customer never has to chase recovery on something that never settled.

The product fits inline with the customer's existing claims processing or payment system, typically as a service function called from a stored procedure or from an inbound webhook. Integration is days, not months. The pricing is up to five million dollars annual flat fee, tiered by transaction volume and product breadth. There is no percentage of recovery, no contingency, and no incentive misalignment. The customer pays for detection and proof. JIL is paid the same whether the customer recovers nothing or everything.

The natural buyer is a payer with high transaction volume and meaningful fraud exposure. Health plans, Medicaid managed care organizations, property and casualty insurers, banks with treasury rails, and federal disbursing agencies are all good fits.

7.2 Retroactive

Forensic recovery on settled claims, with court-ready evidence.

Retroactive performs forensic sweeps on already-settled claims to identify overpayments, ineligible recipients, fraudulent providers, and bad-actor networks. Unlike conventional audit shops, JIL's output is not a finding letter. It is a CREB package, court-ready and admissible under FRE 902(14), that the customer's general counsel can take directly to recovery action or referral.

The product runs in batch mode against millions of historical claims. The forensic catalog is the same one Pre-Settlement uses. The Bad Actor Registry is cross-referenced for every flagged entity, surfacing patterns the customer's own data could not surface in isolation. Every CREB generated by Retroactive is hashed and anchored to CourtChain at generation time. A customer who sits on a CREB for two years, then decides to pursue recovery, can prove that the evidence package existed unmodified at the moment of generation.

Pricing is tiered. Tier one, retroactive scan with detection findings, is a flat fee from one hundred fifty thousand to seven hundred fifty thousand dollars depending on MCO size. Tier two, full investigation with CREB output, is priced per case for the cases the customer chooses to advance.

7.3 Pre-Clearance · Attestyx

Approve grantees, vendors, and counterparties before funds move.

Attestyx is JIL's pre-clearance product, designed for foundations, federal grant programs, and any disbursing entity that wants to prove every recipient was vetted before the wire left. The product is live at `grants.jilsovereign.com`. Identity, beneficial ownership, sanctions screening, and program-eligibility checks run in advance of disbursement. The output is an attestation packet that a general counsel can stand behind in front of a board, an inspector general, or a journalist.

Attestyx fills a gap the philanthropic and federal grants ecosystem has never closed. Every responsible foundation knows it should diligence its grantees. Few have the operational capacity to do so consistently across hundreds of grantees a year. Federal grant programs face the same pressure with much higher volumes and much more political scrutiny. Attestyx makes diligence a workflow rather than an aspiration. Per-grantee clearance fees apply. Volume tiers are available for foundations writing one hundred or more grants per year.

The natural buyers are family foundations, donor-advised fund administrators, federal grant-making agencies, and state administrators of federal pass-through funds. Attestyx is also relevant to procurement teams making vendor decisions in regulated industries.

7.4 Asset Intel

Map the counterparty graph. Surface what is hidden in plain sight.

Asset Intel is the counterparty risk graph engine. It builds and queries the network of relationships between entities, assets, and identities to surface shell company structures, undisclosed beneficial ownership, sanctions exposure, and politically exposed persons. It is the engine behind every Verdict Engine identity and counterparty check, and a standalone product for institutions that need diligence depth.

The product covers OFAC, FinCEN, EU and UK sanctions lists, PEP and adverse-media corpora, and a continuously refreshed beneficial-ownership graph. Network-level exposure mapping surfaces second-order and third-order risk. A live API supports inline risk scoring during onboarding workflows. Pricing is per-query and subscription tiers, with enterprise volume agreements available for high-throughput customers.

The natural buyers are AML and KYC teams at financial institutions, investment firms doing sanctions-sensitive deals, and federal procurement offices vetting awardees and subcontractors.

7.5 Wallet Intel

On-chain plus off-chain wallet attribution at the speed of the rail.

Wallet Intel attributes wallets, addresses, and transaction patterns to real-world entities and known schemes. It surfaces mule networks, laundering layers, sanctioned counterparty exposure, and pre-settlement risk on payouts. Designed to feed the Verdict Engine in real time and to power independent analyst workflows for fraud teams and federal investigators.

The product covers cross-chain attribution across Ethereum, Bitcoin, and major Layer 2 networks, mule-pattern and layering detection, sanctioned-wallet matching, and pre-settlement risk scoring on payouts and transfers. Investigator-friendly graph and timeline views support manual analyst workflows in addition to programmatic scoring.

The natural buyers are banks with crypto exposure, payment processors, exchanges, and federal financial-crimes investigators. Pricing is per-query and subscription tiers, with federal engagement agreements available.

7.6 Utilization Management

Proof beneath the plan's medical team. Never above it.

Utilization Management is JIL's proof layer for prior authorization and medical-necessity decisions. It does not approve or deny care. That is a bright-line scoping decision, made deliberately and reinforced throughout the product's design. The product validates that the medical evidence on file is internally consistent, that the documentation pattern matches peer norms, and that any flagged outliers are surfaced for the human reviewer with a sealed audit trail.

The plan's clinicians make the call. JIL proves what the clinicians had in front of them when they made it. This deliberate scoping is an explicit response to the litigation environment around algorithmic care decisions. The product is positioned as an evidence layer, not a decision layer, and that positioning is reflected in every API, every endpoint, every audit log, and every customer agreement.

The natural buyers are Medicaid managed care plans, commercial health plans, and integrated delivery systems whose UM decisions are subject to litigation, regulatory scrutiny, or member complaint risk. Pricing is annual flat fee tiered by membership size. The product is available standalone or bundled with Pre-Settlement.

PART VIII

Customer *Surfaces.*

Where humans meet the platform. Five surfaces, all anchored to the same L1, all queryable by the same proof system.

8.1 Institutional Portal

SURFACE 01

Portal

portal.jilsovereign.com

For MCOs, federal program offices, state Medicaid directors, and integrated delivery systems.
The institutional portal is the authenticated workspace where customer teams operate the platform. It contains a transaction analytics view (TAVE), a cluster explorer for inspecting entity networks, a profile selector for switching between operating units in multi-entity organizations, an execution dashboard for monitoring service health, and a CREB library where every evidence package the customer has generated is searchable by case identifier, date range, or counterparty.

The portal is the daily-driver surface for compliance officers, fraud analysts, recovery teams, and audit liaison staff. It is also where the customer's own auditors come when they want to see exactly what JIL did, and what JIL surfaced, on any specific case.

8.2 Attestyx · The Grants Surface

SURFACE 02

Attestyx

grants.jilsovereign.com

For foundations, federal grant offices, and pass-through fund administrators.
Attestyx is the customer-facing surface of the Pre-Clearance product. It presents grant programs, grantees, and clearance status as a single workflow. A program officer can submit a prospective grantee for clearance, receive an attestation packet, and forward that packet to the disbursement system. Every attestation is anchored to CourtChain. A foundation that grants ten million dollars to a hundred grantees in a year accumulates a hundred portable attestations the foundation's general counsel can produce on demand.

The site has a public marketing surface and an authenticated workspace. The marketing surface is designed for foundation presidents and federal grant administrators researching the platform. The workspace is designed for the program officers who use it daily.

8.3 Treasury Wallet · Corporate Surface

SURFACE 03

Treasury Wallet

`wallet.jilsovereign.com`

For corporate treasurers, CFOs, and bank operations teams.
The treasury wallet is the corporate-facing surface that lets a CFO or a bank's treasury operations team initiate, screen, and settle outbound payments under JIL pre-settlement screening. Every payment passes through the Verdict Engine. Every cleared payment receives a PoCS receipt. Every blocked payment lands in Sealed Escrow pending the customer's resolution workflow.

The treasury wallet is multi-currency, multi-rail, and integrates with the customer's existing core banking platform through standard payment messages. The product is positioned for institutions that need cryptographic proof of pre-settlement diligence at scale, particularly cross-border treasury operations where sanctions exposure and beneficial ownership questions accumulate quickly.

8.4 Consumer Wallet · Retail Surface

SURFACE 04

Consumer Wallet

`getjil.com · wallet.getjil.com`

For individual token holders, retail members, and consumer participants in the JIL network.
The retail surface is the consumer-facing presence of the JIL network. It hosts the public token sale, the consumer wallet application, and the retail-grade introduction to the platform. The retail surface is operated under the `getjil.com` brand to maintain a clean separation from the institutional `jilsovereign.com` properties. Institutional customers see one set of materials. Retail participants see another. The underlying L1 is the same.

The retail wallet supports stablecoin and fiat funding, peer-to-peer transfer subject to the same Verdict Engine the institutional products use, and a transparent ledger of every action the user has taken on the platform. The user is the controller of their own keys, with optional recovery flows for users who prefer custodial convenience.

8.5 RUWI · The Developer Surface

SURFACE 05

RUWI API

`ruwi.jilsovereign.com`

For developers and product teams embedding payment integrity into their own applications.
RUWI is JIL's developer-first payment integrity API. It exposes the Verdict Engine through a clean three-tier API surface that developers can integrate into a payment flow, an onboarding workflow, or a wallet application without standing up a full institutional deployment. Tier one is detection at five basis points per check. Tier two is full 175-check

verification with CREB output. Tier three is forensic engagement, scoped to the customer's specific case.

RUWI's architecture is locked. There is no money transmission license requirement because RUWI does not custody money. USDC and USD prepaid balances are held in segregated accounts. The product supports both Mode A passive attestation and Mode B active enforcement, depending on the developer's posture.

PART IX

Three deployment options.

Same six product lines. Same evidence anchor. The customer picks the runtime.

JIL ships as containerized services. Where those containers run is the customer's decision. We support three first-class deployment paths today, designed to meet customers where their existing data infrastructure already lives.

OPTION 01

Snowflake

Snowpark Container Services. Native data sharing. Horizon Catalog governance. Per-warehouse compute. Best fit for customers standardized on Snowflake who want fastest path to value.

OPTION 02

Databricks

Databricks Apps. Delta Lake substrate. Unity Catalog governance. Photon and serverless SQL. Best fit for lakehouse-native, ML-heavy customers running Unity Catalog.

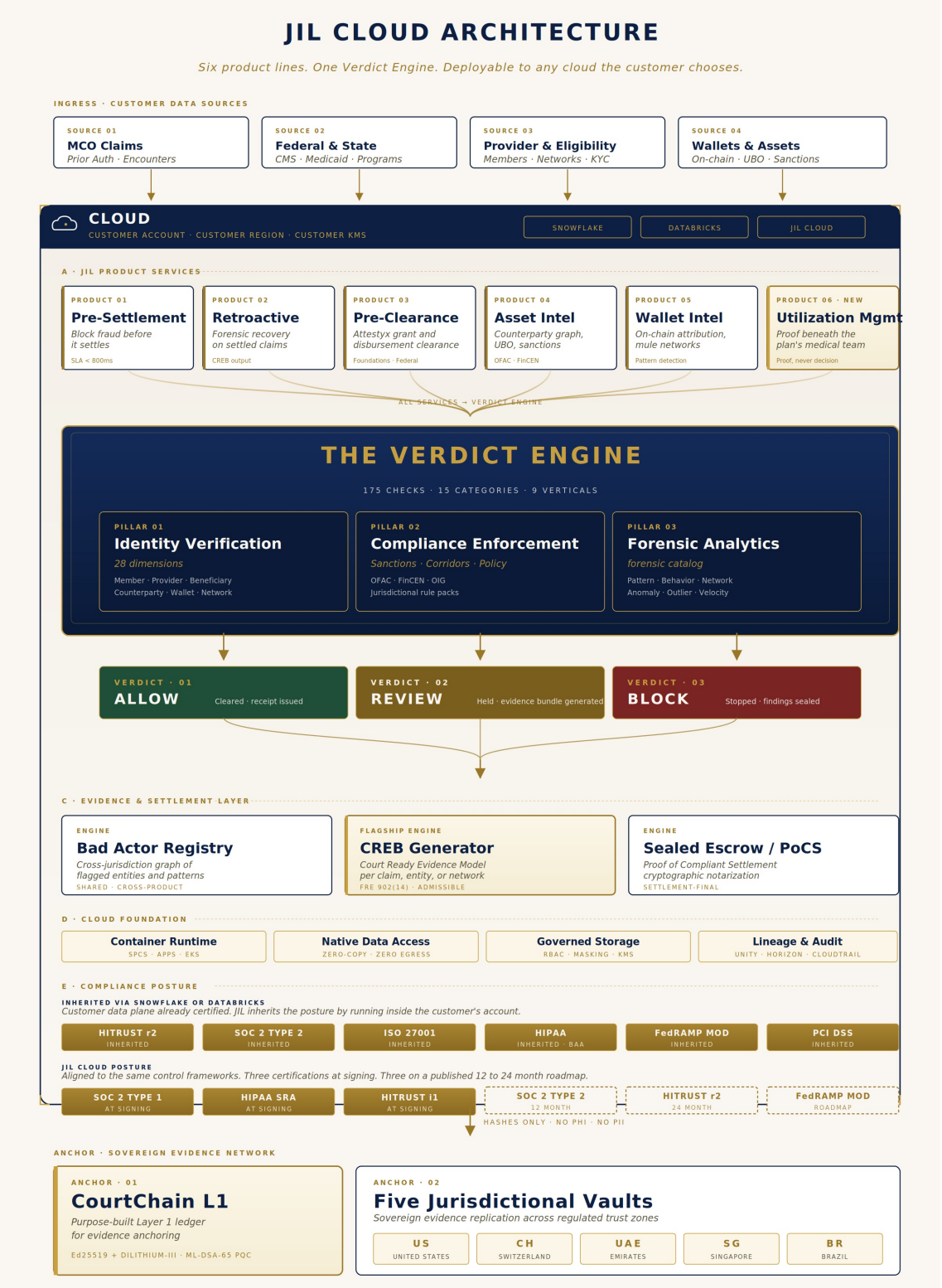
OPTION 03

JIL Cloud

Amazon EKS. PrivateLink. KMS, IAM, GuardDuty. Customer VPC or peered. Best fit for heterogeneous estates, federal customers, and any institution requiring maximum control.

The three options share the same JIL services, the same Verdict Engine, the same CREB output, and the same anchor to CourtChain. What differs is the substrate. A customer running on Snowflake inherits Snowflake's certified compliance posture, Snowflake's native data access primitives, and Snowflake's billing relationship. A customer running on Databricks inherits the same from Databricks. A customer running on JIL Cloud takes on more direct operational responsibility but gains maximum control, including the option of full air-gap deployments for federal use cases.

FIGURE 2 · CLOUD ARCHITECTURE



The same architecture renders identically across Snowflake, Databricks, and JIL Cloud. Six product lines feed one Verdict Engine. The engine emits Allow, Review, or Block. Evidence layer outputs anchor to CourtChain. The cloud foundation is the customer's choice.

The trust boundary.

What runs inside the customer's cloud, and what stays sovereign.

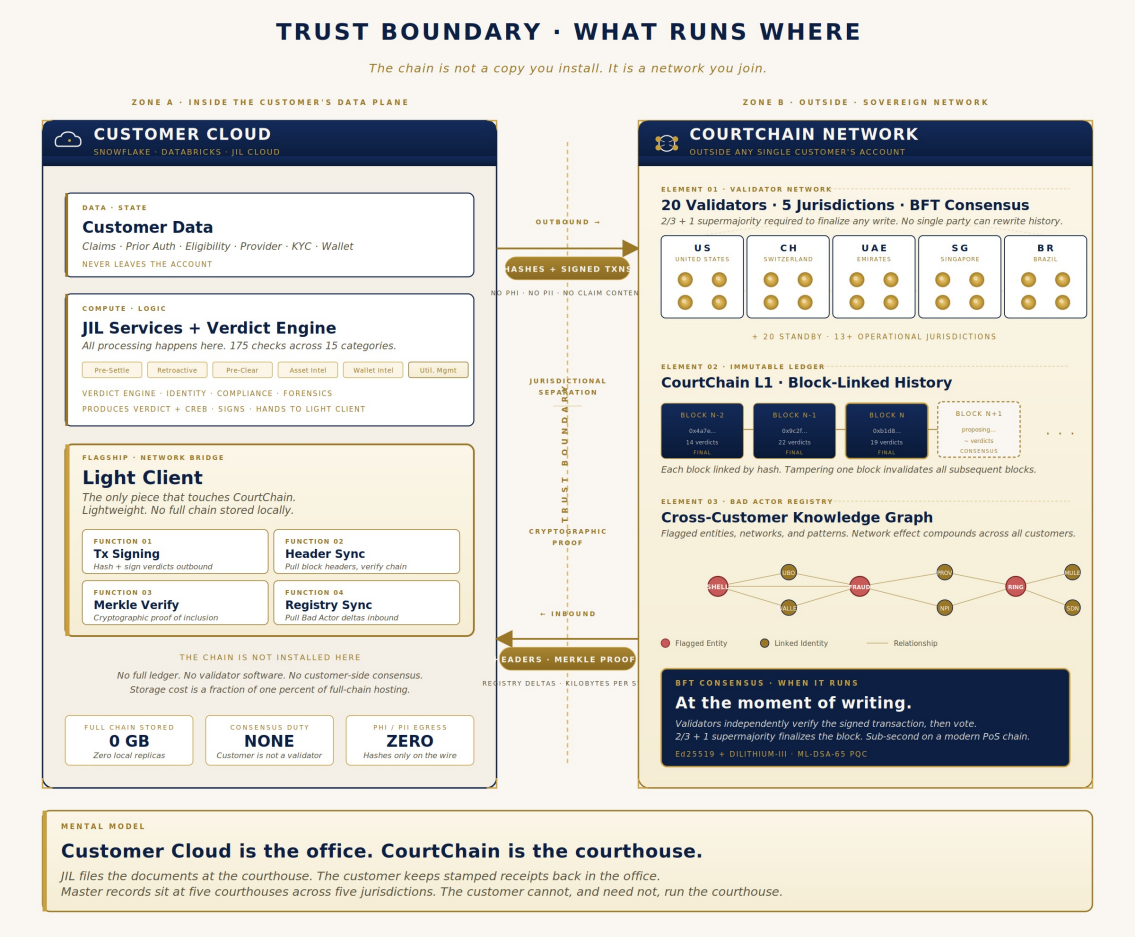
The platform's most important architectural property is also its most easily misunderstood. Customer data never leaves the customer's cloud. JIL's intellectual property never enters it in inspectable form. Cross-customer intelligence never replicates into any single customer's environment. These three invariants are enforced by the trust boundary.

Inside the customer's cloud, the customer holds the data and runs the JIL services. The customer's compute pool runs the JIL containers. The customer's storage holds the customer's claims, prior authorizations, member records, and provider directories. The customer's KMS encrypts everything at rest. The customer's authentication system controls who logs in. The customer's existing audit and governance tooling sees every action JIL takes against the customer's data.

Outside the customer's cloud, on JIL's sovereign network, sits the Authority Server, the Bad Actor Registry, the CourtChain L1 ledger, and the build-and-sign pipeline that produces JIL's container images. The cross-customer graph never replicates to any single customer. The chain itself is run by validators in five jurisdictional vaults, none of them under the customer's authority and none of them under JIL's unilateral authority either.

The two halves communicate over a customer-approved network egress allow-list of four FQDNs. Hashes leave. Signed verdicts leave. Registry queries leave. Customer data does not leave. JIL's source code does not enter. The cross-customer graph does not enter. The figure on the next page makes the boundary explicit.

FIGURE 3 · TRUST BOUNDARY



The chain is not a copy you install. It is a network you join. Customer Cloud is the office. CourtChain is the courthouse.

PART XI

IP protection: defense in depth.

Seven independent layers between the customer's account administrator and JIL's intellectual property. Each one defeats a different attack.

JIL is in production inside customer cloud accounts where the customer's account administrator has elevated visibility into the runtime. That posture is normal for any vendor running services inside a customer's environment, and it is what makes Snowpark Container Services, Databricks Apps, and EKS commercially viable for vendors at all. What it requires is a deliberate layering of controls that protect the vendor's intellectual property without restricting the customer's ability to audit what is happening on their own infrastructure.

JIL's posture is defense in depth. Seven independent layers. Each one defeats a different attack vector. They compound. An attacker would need to defeat all seven simultaneously to reconstruct the platform. To our knowledge, no commercially deployed engine on the

market has this combination of protections in place.

LAYER	MECHANISM	WHAT IT DEFEATS
L1	Stripped Rust binary, link-time optimized, no symbols	Source-level reverse engineering with conventional decompilation tools.
L2	AES-256-GCM encrypted rule packs at rest in image	Image extraction. A pulled and saved image yields ciphertext, not logic.
L3	Authority-mediated runtime attestation, 5-minute key TTL	Offline replay. The image cannot run disconnected from JIL Authority.
L4	In-memory only decryption, never on disk, never in logs	Filesystem inspection, log scraping, environment variable dumping.
L5	Cosign image signature verification on every pull	Image substitution. Tampered binaries fail to start.
L6	Network egress allow-list, four FQDNs only	Data exfiltration concerns from both directions.
L7	Cross-customer data and the L1 ledger stay on JIL infrastructure	Moat extraction. The most valuable IP physically does not exist on the customer side.

NET EFFECT

An attacker with full account administrator access reads a stripped binary, dumps encrypted blobs they have no key for, watches a network whose egress is locked to four hostnames, and after revoking JIL Authority access, finds that the engine no longer runs.

PART XII

Compliance posture.

Aligned to every framework that matters. Inherited where possible. Independently certified where it must be.

JIL's compliance posture follows a clear philosophy. Where the customer has already standardized on a certified data platform, JIL inherits the platform's posture by running inside it. Where JIL operates its own platform, JIL stands on its own controls. In both cases, the underlying control framework is the same set of internationally recognized standards, mapped to NIST CSF 2.0 across Govern, Identify, Protect, Detect, Respond, and Recover.

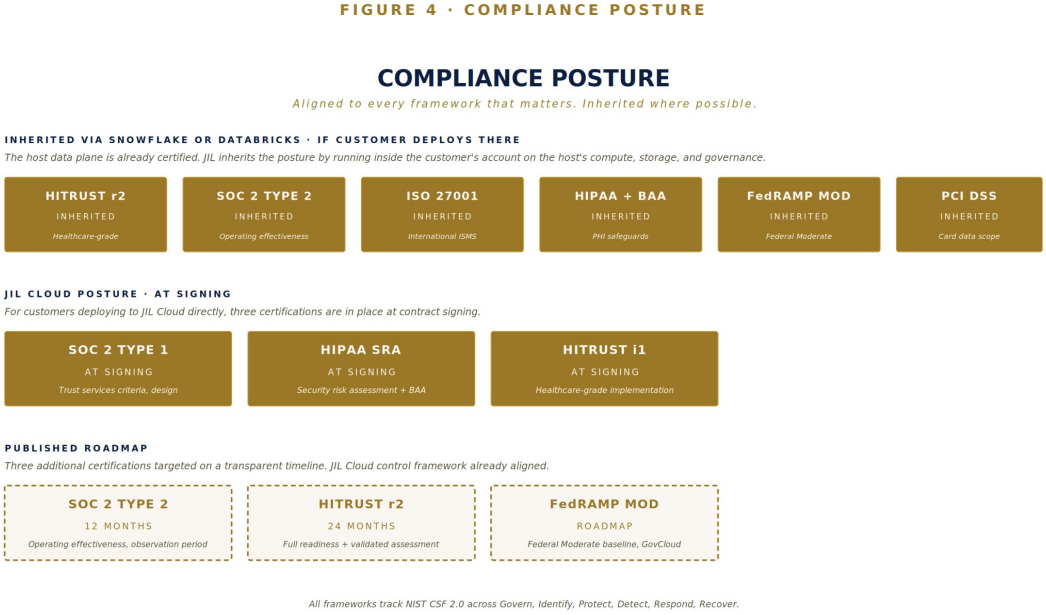
Inheritance via Snowflake or Databricks

A customer who deploys JIL on Snowpark Container Services inside their Snowflake

account inherits Snowflake's certified posture as the substrate for JIL's deployment. The same applies to Databricks customers running JIL on Databricks Apps. The certifications cover HITRUST r2 for healthcare-grade controls, SOC 2 Type 2 for operating effectiveness, ISO 27001 for international information security management, HIPAA with Business Associate Agreement for protected health information, FedRAMP Moderate for federal authorization, and PCI DSS where card data is in scope. JIL's services run inside that certified perimeter. The customer's auditors run their existing tooling against JIL exactly as they would any other native workload.

JIL Cloud direct deployment

For customers who deploy to JIL Cloud directly on Amazon EKS, JIL stands on its own. At contract signing, JIL Cloud is independently aligned with three certifications: SOC 2 Type 1 for trust services criteria design, HIPAA Security Risk Assessment with an executable Business Associate Agreement, and HITRUST i1 for healthcare-grade implementation. The roadmap to full certification is published and tracks twelve to twenty-four months for the remaining frameworks.



Six certifications inherited via the customer's existing data platform. Three at signing on JIL Cloud. Three on a published twelve to twenty-four month roadmap. All mapped to NIST CSF 2.0.

PHI and PII handling

JIL is engineered around a strict PHI and PII discipline. The CourtChain ledger never carries protected health information or personally identifying information. Hashes only on the wire. Inside the customer's data plane, JIL services operate on PHI and PII under the customer's existing governance. JIL does not pull customer data into JIL infrastructure. JIL does not maintain copies of customer data outside the customer's account. The Bad Actor Registry, which JIL operates, contains entity-level signals contributed by customers in pre-hashed and entity-scoped form before submission. The registry never holds raw transactional data.

NIST CSF 2.0 alignment

JIL's internal control framework is mapped to NIST CSF 2.0 across all six core functions. A self-assessment sign-off document exists, covering Govern (organizational context, risk management strategy, supply chain risk), Identify (asset management, risk assessment, improvement), Protect (identity management, awareness training, data security, platform security, technology infrastructure resilience), Detect (continuous monitoring, adverse event analysis), Respond (incident management, analysis, response reporting and communication, mitigation), and Recover (incident recovery plan execution, recovery communication). Maturity ratings range from Tier 1 to Tier 4 across the assessed functions, with documented improvement plans for any function below the customer-required tier.

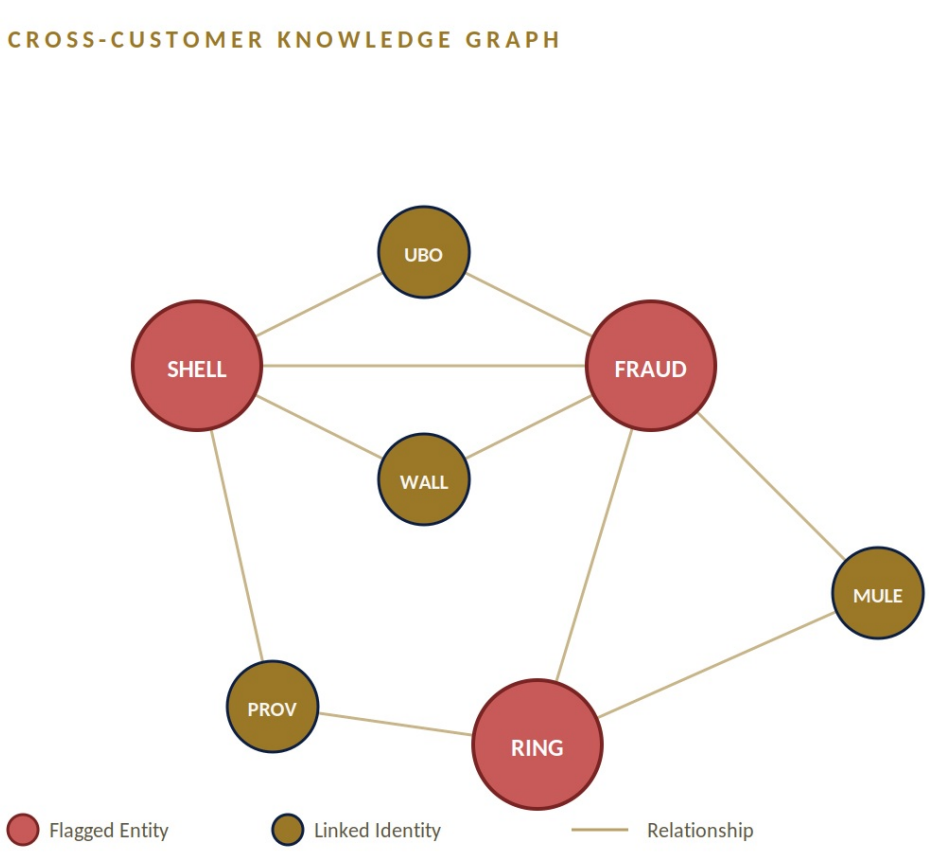
PART XIII

The Bad Actor Registry.

The shared knowledge graph. The compounding network effect. The moat.

The Bad Actor Registry is the most consequential network-effect property of the JIL platform. Every flagged entity, every linked wallet, every detected pattern is added to a graph that all customers query and all customers contribute to. A fraud ring caught at one MCO surfaces in milliseconds at every other MCO, every federal agency, and every foundation on the network. The registry is the long-term moat. The longer JIL runs, the more entities are flagged, the more relationships are mapped, the harder it becomes for a bad actor to operate anywhere on the network without being recognized.

FIGURE 5 · CROSS-CUSTOMER KNOWLEDGE GRAPH



A schematic of the registry. Red nodes are flagged entities. Gold nodes are linked identities. Edges are observed relationships. The real graph spans hundreds of thousands of nodes and grows continuously.

The registry is operated on JIL infrastructure, not replicated into customer environments. This is a deliberate design property. If the registry replicated to every customer, every customer would hold a copy of every other customer's contributed intelligence. That property is incompatible with the contractual and regulatory commitments customers expect their vendors to honor. By keeping the registry on JIL infrastructure and exposing only per-query access, JIL preserves the network effect for all customers while protecting each customer's contributions from broad exposure.

Customer queries against the registry are rate-limited, logged, and per-entity scoped. There is no bulk download interface. There is no dataset export. There is no mechanism by which a single customer can extract the registry. The customer gets the answer they need for the verdict they are evaluating, and nothing more.

> *Every customer on the network strengthens every other customer's defenses. The compounding is real and it accelerates.*
>
> NETWORK EFFECT

PART XIV

Proof of execution.

We did not draw this up. We built it. Here are the receipts.

JIL has been under construction for approximately two and a half years. The platform is in production today. What follows is the public-facing summary of what has been built. We share it because the institutional reader is right to demand evidence that the architecture above is more than a thesis.

300
PRODUCTION SERVICES

1.5M
LINES OF CODE

75
PATENTS FILED

175
CHECKS · 9 VERTICALS

9
OPERATIONAL VERTICALS

10
LIVE VALIDATORS

5
JURISDICTIONAL VAULTS

13+
OPERATIONAL JURISDICTIONS

What this means in practice

Three hundred production services means JIL is a real distributed system, not a marketing artifact. One point five million lines of code means the platform is engineered, audited, and operationally complete in a way that two engineers and a notebook cannot match. Seventy-five patents filed means the underlying methods are protected and that JIL has institutional credibility with patent counsel. One hundred and seventy-five attestation checks deployed across nine verticals means the Verdict Engine has the catalog depth and

the operational breadth that meaningful payment integrity at scale requires.

Ten live validators today, scaling to twenty active and twenty standby, distributed across thirteen or more operational jurisdictions, anchored to five sovereign vaults, means CourtChain is a working blockchain network rather than a planned one. We have run validators in production for long enough to have encountered, diagnosed, and resolved the operational issues that any blockchain network encounters at scale.

Representative milestone: Medicare audit

In one representative engagement, the Retroactive product processed forty-nine point eight seven million Medicare records in seventeen minutes and surfaced eight point three million dollars in recoverable findings, packaged as CREB. The volume and the time-to-result are not the headline. The headline is that the eight point three million dollars came back not as a finding letter but as admissible evidence packages that could walk into a recovery action without further preparation.

> **BOTTOM LINE**
>
> *JIL is in production. The architecture above is the architecture of a working platform, not a planned one. The receipts are public, the patents are filed, the validators are live, and the customers are real.*

PART XV

The mission.

Trust, restored. Ten percent at the protocol level, dedicated to human flourishing in perpetuity.

JIL exists for a commercial reason and a moral one. The commercial reason is that the institutional payment integrity market is large, growing, and structurally underserved. The moral reason is that finance lost its grip on trust at scale, and someone has to put it back. Both reasons are real. Both motivate the work.

The Human Flourishing Mandate

JIL's protocol allocates ten percent of the network's profits to a Human Flourishing Mandate, encoded at the protocol level. The allocation is not a marketing program. It is an architectural commitment. It cannot be removed by future executives, future investors, or future board configurations without changing the protocol itself, which the validator network would not ratify.

The mandate funds initiatives at the intersection of payment integrity and human dignity: clean disbursement infrastructure for humanitarian aid, fraud-resistant rails for grant programs serving the most vulnerable, and capacity building for the regulators and inspectors general whose work the platform is designed to support. The thesis is that proof and dignity are linked. A payment system that cannot prove what it did is a system that cannot serve the people who depend on it. We are building the proof.

Closing

This document has tried to be complete without being exhausting. The architecture above is what is built. The products above are what is shipping. The compliance posture above is what is in place. The validators above are what is running. The mission above is what we are accountable to.

If you are reading this as a chief information officer, your next conversation is about the deployment option that fits your environment. If you are reading this as a general counsel, your next conversation is about the CREB output and FRE 902(14). If you are reading this as a foundation president or a federal grants administrator, your next conversation is about Attestyx. If you are reading this as an investor, your next conversation is about the network effect.

In every case, your next conversation is one we are ready to have.

READY TO BEGIN

Detection in front. Proof behind. Anchored in five sovereign jurisdictions. Built to put trust back into finance. Visit jilsovereign.com/connect to schedule a conversation.

INSTITUTIONAL

jilsovereign.com

Portal · TAVE · CREB Library

GRANTS · ATTESTYX

grants.jilsovereign.com

Foundations · Federal grant offices

TREASURY · RETAIL

wallet.jilsovereign.com

getjil.com · wallet.getjil.com

CONNECT

jilsovereign.com/connect

support@jilsovereign.com