



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

WHITE PAPER: THE VERIFIED TRUTH ECONOMY

From Debt-Based Serfdom to Sovereign Asset Capitalization

Author: Eddie Elam, Principal Architect, IDIA Data Inc.

Subject: The Structural Obsolescence of the Mortgage-Backed Standard and the Rise of Verified Truth as a Utility, establishing the Universal Basic Asset (UBA).

READER ORIENTATION: The IDIA Protocol is a real-time diagnostic utility that measures operational and system readiness to prevent failure in high-consequence environments. Every index within this protocol functions exclusively as an objective telemetry gauge for immediate operational stability, occupational safety, and enterprise risk mitigation.

ABSTRACT

The global digital economy has entered the "Post-AI Era," characterized by an "AI Slop" flood of synthetic content that creates a crisis of reality. The foundational logic of the "Attention Economy" has eroded; the primary scarcity is no longer information, but Verified Provenance. Simultaneously, the global financial system faces a solvency crisis driven by the liquidity trap of the Mortgage-Backed Economy (MBE).

IDIA Data Inc. provides the foundational data infrastructure for the digital economy by establishing an institutional protocol for data registration, auditable consent management, commercial licensing administration, cryptographic provenance, and programmatic royalty distribution for eligible data assets. Orchestrated across client-facing nodes (*Life by IDIA* for individual contributors and *IDIA Pay* for merchants) and an enterprise procurement desk (*The IDIA Hub*), the platform utilizes the proprietary IDIA Synapse Engine to convert verified, zero-PII operational and behavioral telemetry into structured, marketable data products. Rather than asserting abstract ownership over ambient information, the IDIA Protocol establishes an auditable administrative agency model: contributors document clear permissions and grant defined commercial licenses over their qualifying data contributions, enabling institutional buyers to ingest legally indemnified ground-truth datasets while automatically remitting performance-based royalties directly to the originating contributors.



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

Table of Contents

EXECUTIVE SUMMARY & INVESTOR THESIS	3
THE STRUCTURAL DATA ASYMMETRY: EXTRACTION WITHOUT ATTRIBUTION	7
DATA RIGHTS, ADMINISTRATIVE AGENCY, AND CONSENT	24
DATA PRIVACY, SECURITY & RE-IDENTIFICATION	32
COMMERCIAL MODEL & ENTERPRISE LICENSING	41
ROYALTY ECONOMICS & FINANCIAL SETTLEMENT	48
TOKENOMICS & TREASURY DESIGN	58
DATA-AS-PERFORMANCE FRAMEWORK	64
THE HUMAN RELIABILITY INDEX & SENSITIVE DATA	68
MARKET, COMPETITION, AND GO-TO-MARKET STRATEGY	72
BUSINESS MODEL, FORECASTS, & ANGEL INVESTMENT	78
LEGAL, REGULATOR, AND GOVERNANCE DISCLOSURES	84
MACROECONOMIC & SOCIETAL IMPLICATIONS	89
ANNEX I: QUANTITATIVE FINANCIAL MODEL	91



Section 1

EXECUTIVE SUMMARY & INVESTOR THESIS

1.1 Rights Administration & Performance Royalties: The Music Publishing Blueprint

To understand the commercial and operational mechanics of the IDIA Protocol, the platform operates on an established business-model framework: **music publishing administration and performance rights collectives**.

In the music ecosystem, administrative agents and collective management organizations (such as ASCAP, BMI, or SoundExchange) act on behalf of songwriters and master-rights holders whenever a composition is broadcast, streamed, or synchronized—maintaining a centralized, registered repertoire of works, tracking commercial usage across distribution channels, collecting licensing fees from commercial broadcasters, and programmatically distributing fractional performance royalties back to the documented rights holders.

IDIA applies this exact operational logic to the data economy:

- **Repertoire Registration:** Individual and business contributors register their qualified data sources, documenting permissible licensing categories, restrictions, and explicit consent boundaries.
- **Commercial Licensing Administration:** Operating as an exclusive Authority of Record and administrative licensing agent, IDIA makes these verified, zero-PII data catalogs available to enterprise buyers, AI platforms, and algorithmic systems through structured query endpoints and marketplace bundles.
- **Performance-Based Settlement:** When an enterprise buyer queries or consumes a data asset, the transaction functions identically to a digital public performance, triggering an automated financial split that deposits licensing revenue into the ecosystem and routes programmatic royalties directly to the contributing nodes.

Legal Distinctions and Boundaries:

This framework serves strictly as a **commercial business-model and accounting analogy**. IDIA fully recognizes raw data telemetry streams do not enjoy statutory copyright protections equivalent to musical works or sound recordings (*Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 1991). Raw ambient data, spatial observations, and machine exhaust are non-copyrightable facts. IDIA's administrative agency derives entirely from enforceable, bilateral contract law, verified consent records, secure technical access controls, and commercial



data licensing agreements. Contributors earn compensation through contractual performance yields generated when an authorized enterprise consumes their verified, aggregated ground truth.

1.2 The Commercial & Investment Opportunity

IDIA Data Inc. bridges the widening gap between enterprise artificial intelligence demand and compliant data procurement. As statutory privacy enforcement escalates and unverified web scraping degrades machine learning performance, enterprise data buyers face severe liability and operational disruption. IDIA addresses this market failure through a compliant data utility protocol anchored by verified provenance, auditable consent ledgers, and programmatic performance royalties.

The Enterprise Need & Target Customers

IDIA directly targets four high-consequence enterprise verticals requiring clean, verifiable ground-truth datasets with zero Personally Identifiable Information (PII):

- **Algorithmic Trading & Quantitative Desks:** Financial institutions requiring microsecond-latency operational telemetry and consumer velocity feeds to generate market alpha.
- **Frontier AI & Machine Learning Developers:** Foundation model developers and enterprise labs requiring cryptographically authenticated human telemetry to prevent model collapse and synthetic data poisoning.
- **Enterprise Insurers & Logistics Operators:** Risk underwriters seeking dynamic human and fleet operational readiness metrics—governed by the Human Reliability Index (HRI)—to accurately price commercial liability and workers' compensation coverage.
- **Regulated & Public Sector Infrastructure:** Mission-critical enterprise and municipal entities requiring immutable audit logging, sovereign data environments, and verified provenance workflows.

Dual-Engine Monetization Model

The protocol deploys a resilient "Double-Helix" revenue architecture that pairs high-margin recurring software subscriptions with scalable, consumption-based data clearing fees:

- **The Floor (Transactional Utility & DaaS Consumption):** Enterprise data access through *The IDIA Hub* is monetized via annual platform subscriptions (Analyst Tier at \$9,995/year to Enterprise Tier at \$49,995+/year) combined with metered Synapse Credit consumption (\$0.75 per credit) for real-time feature feeds and query execution.



Secondary transactional revenue is generated via low-friction merchant settlement fees and standard off-ramp processing (1.5%).

- **The Ceiling (Cognitive Optimization SaaS):** High-margin recurring software subscriptions monetizing personal and merchant operational intelligence across tiered offerings, including *Life Pro* (\$9.99/month), *Life Pro+* (\$49.99/month), *Pure Alpha* (\$99.99/month), and *IDIA Pay Pro* (\$49.99/month).

Competitive Differentiation: The Compliance & Provenance Moat

While traditional data brokers rely on opaque, non-consented web scraping and commoditized fintechs offer isolated payment terminals, IDIA delivers an integrated, legally defensive architecture:

- **Auditable Consent Lineage:** Every data asset is bound to an immutable cryptographic consent hash, ensuring strict compliance with evolving state, federal, and international privacy mandates.
- **The Liability Shield & Indemnity Reserve:** Qualified enterprise transactions are backed by a contractual liability shield supported by the bankruptcy-remote *IDIA Indemnity Reserve, LLC*, offering institutional buyers indemnification against third-party provenance claims.
- **Edge-Processed Zero-PII Guarantee:** Raw identifiers remain securely isolated on local device hardware; only zero-knowledge proofs and mathematically cleansed aggregates are transmitted to the marketplace.

Demonstrated Milestones vs. Market Hypotheses

To maintain institutional rigor, IDIA explicitly separates verified operational traction from long-term scaling projections:

- **Demonstrated Operational Traction (Production & Pilot):**
 1. Native consumer application (*Life by IDIA*) deployed and available on the iOS App Store.
 2. Enterprise marketplace portal (*The IDIA Hub*) launched in active webapp beta with live data catalog endpoints.
 3. Governance and economic smart contracts deployed on the Base Layer-2 network with liquidity pools established on Uniswap.



4. Strategic technology collaborations established, including an Independent Software Vendor (ISV) partnership with Zebra Technologies and regional pilot infrastructure in Louisville, Kentucky.
- **Market Hypotheses (Scaling Roadmap):** Projections regarding rapid merchant roll-ups, multi-state Money Transmitter License (MTL) expansion, and hyperscale API adoption represent modeled growth targets subject to capital availability, market reception, and regulatory execution.

1.3 Seed Capital Deployment & Use of Proceeds

IDIA is raising \$10,000,000 in Seed funding via a Simple Agreement for Future Equity ([FIN-SAFE-2026-B]) and accompanying Token Warrant Agreement (SAFE Note Addendum) structured with a \$40,000,000 pre-money valuation cap to fund an 18-to-24-month execution runway:

- **Technology & Product Development (40% | \$4,000,000):** Finalizing core engineering across *Life by IDIA*, *IDIA Pay*, and *The IDIA Hub*, securing dedicated cloud infrastructure, and operationalizing the LangGraph AI multi-agent orchestration layer.
- **Regulatory Compliance & Licensing (20% | \$2,000,000):** Capitalizing Phase 1 Money Transmitter License (MTL) applications, securing required state surety bonds, and formalizing federal compliance programs.
- **Pilot Execution & Merchant Acquisition (15% | \$1,500,000):** Executing the Louisville regional pilot, onboarding initial paid merchant partners, and validating zero-CAC contributor acquisition funnels.
- **Liquidity & Treasury Reserves (15% | \$1,500,000):** Establishing required payment processing liquidity, capitalization reserves, and operational contingency buffers.
- **Operations & General Administration (10% | \$1,000,000):** Executive leadership, core legal and accounting retainers, regulatory counsel, and operational overhead.

This capitalized foundation de-risks the core protocol, validating the commercial data flywheel in a controlled regional market before initiating national Series A scaling.



Section 2

THE STRUCTURAL DATA ASYMMETRY: EXTRACTION WITHOUT ATTRIBUTION

The global digital economy operates on a foundational market distortion: individuals and commercial enterprises generate the telemetry, behavioral patterns, and operational signals that power enterprise intelligence and frontier artificial intelligence models, yet they remain entirely disenfranchised from its downstream monetization. Under current commercial architectures, high-value human and organizational data is harvested passively without continuous provenance, granular consent, or programmatic compensation.

Simultaneously, enterprise data buyers face an escalating integrity crisis. Ingesting opaque, scraped datasets exposes institutional buyers to severe statutory liabilities under expanding privacy frameworks, while poisoning artificial intelligence training pipelines with unverified synthetic noise. The market lacks a standardized infrastructure that bridges this divide—one that enables contributors to systematically register eligible data assets, verify ongoing consent, and participate in performance-based licensing royalties, while providing enterprise consumers with an auditable, legally indemnified stream of verified ground truth.

2.1 The Macroeconomic Solvency Crisis: Asset Mismatch, Debt Traps, and Liquidity Latency

1. **The Asset Mismatch (The 92% Illusion)** The modern economy fundamentally mis-prices human and digital capital by insisting on physical collateral. According to Ocean Tomo's recent Intangible Asset Market Value Study, the balance of value has entirely inverted over the last half-century.

Chart 1: S&P 500 Market Value Composition (Tangible vs. Intangible)

Year	Tangible Assets (Physical/Concrete)	Intangible Assets (IP, Data, Software)
1975	83%	17%
1995	32%	68%
2015	16%	84%
2025	8%	92%

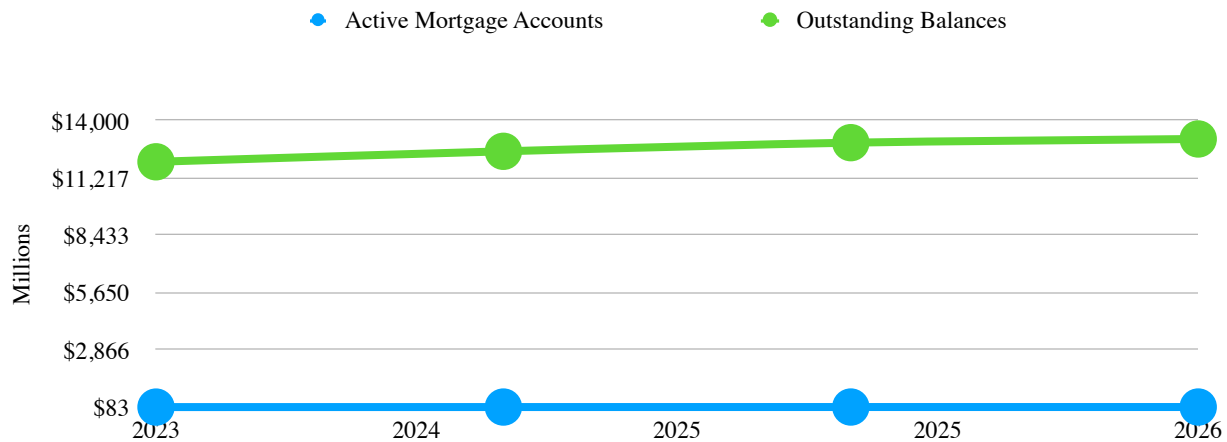
(Source Data: Ocean Tomo 2025 Intangible Asset Market Value Study)

Despite 92% of corporate value originating from intangible, fluid, and cognitive assets (software, data, patents, proprietary formulas), the legacy financial underwriting system predominantly

demands 19th-century physical assets (real estate) to secure capital. The IDIA Protocol rectifies this by turning verified human data streams into a liquid, intangible asset.

2. **The Liability Trap (\$13.12 Trillion in Stagnant Capital)** Homeownership is marketed as wealth accumulation, but structurally, it operates as an engineered debt obligation. As of Q2 2026, U.S. consumers owe a staggering \$13.12 Trillion in outstanding residential mortgage debt, accounting for roughly 70% of all consumer debt.

Chart 2: U.S. Residential Mortgage Debt Balance Expansion



(Source Data: Federal Reserve Bank of New York / Equifax Panel, Q2 2026)

Under the legacy system, the homeowner is effectively merely a "User" of the bank's capital, paying compounded interest for the privilege of shelter. The asset itself generates no active yield; its value relies entirely on speculative market appreciation. The IDIA Home Node flips this: an actively occupied home generates data yield through the Synapse Engine, turning the liability into an active revenue-generating center.

3. **The Liquidity Gap: 45 Days vs. Microseconds** The ultimate failure of the physical standard is *velocity*. Even if a homeowner possesses equity, extracting it is an archaic, friction-heavy process.



Chart 3: Capital Velocity & Extraction Latency Comparison

Capital Extraction Method	Average Processing Time	Institutional Friction
Autonomous AI Agent Trade	< 1 Microsecond	Near Zero
Traditional Equities Sale (T+1)	24 Hours	Low (Broker Fees)
Streamlined Mortgage Refinance	10–15 Days	Moderate
Standard Home Equity Loan (HELOC)	39–45 Days	High (Appraisals, Verification)
Complex Cash-Out Refinance	60+ Days	Severe (Title, Manual Underwriting)

(Source Data: National Mortgage Averages, Q3 2026)

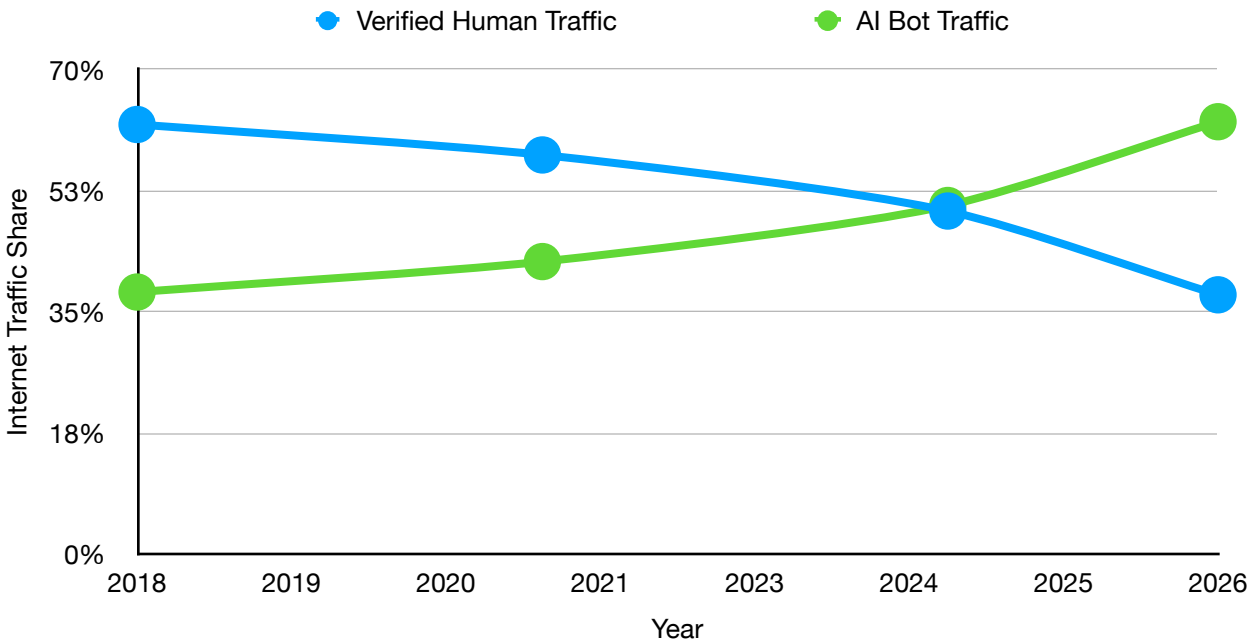
In 2026, the average time to successfully close a Home Equity application (HELOC) or standard refinance takes roughly 39 to 45 days due to manual underwriting, appraisals, and legal checks. In an "Agentic Economy" where AI models trade, allocate, and deploy capital in milliseconds, a 45-day latency window is a fatal inefficiency. Dead capital starves an algorithmic economy of the liquidity it requires to function safely.

2.2 The Information Failure: AI Slop & The Death of Digital Trust

While the asset market freezes, the information ecosystem is experiencing total epistemic collapse. The internet is drowning in "AI Slop" —a self-replicating flood of synthetic content, deepfakes, and dirty data. The fundamental fabric of digital reality is distorted, creating an urgent, quantifiable crisis across three vectors:

1. **The Bot-Traffic Singularity** With the explosion of autonomous web scrapers, synthetic media generators, and LLM-driven agents, the majority of network bandwidth is no longer human.

Chart 4: Global Internet Traffic Composition (Human vs. Bot)



(Source Data: Aggregated Cybersecurity & Bot Traffic Reports, 2026)

When over 60% of the internet is synthetic noise, the legacy web analytics model collapses. Advertisers, platforms, and enterprises are currently paying human-level premiums for interactions generated by algorithms, resulting in catastrophic capital misallocation.

- The Deepfake Economic Drain** We are witnessing an exponential rise in deepfake fraud and biometric spoofing, alongside a wave of catastrophic data hacks that poison the very training sets AI models rely on. The cost of synthetic identity fraud and deepfake impersonation has severely degraded institutional trust.

Chart 5: Escalation of Synthetic Identity & Deepfake Financial Fraud

Vector	2022 Cost (Global)	2026 Projected Cost (Global)	Growth Factor
Synthetic Identity Fraud	\$2.4 Billion	\$14.8 Billion	~6.1x
Deepfake KYC / Biometric Spoofing	\$450 Million	\$6.2 Billion	~13.7x
Enterprise Impersonation (BEC)	\$2.7 Billion	\$9.5 Billion	~3.5x

(Source Data: Interpol / Identity Theft Resource Center Analysis, 2026)



2. **The "Model Collapse" Event** The ultimate consequence of AI Slop is "Model Collapse." When algorithms train on recycled bot traffic and dirty data, they begin to hallucinate exponentially, losing their grip on objective reality. Consequently, the enterprise market is desperately pivoting. "Ground Truth"—data irrefutably anchored to a biological human—has become the most scarce and valuable commodity on earth.

Chart 6: The Data Premium (Value per Terabyte)

Data Classification	2024 Market Value	2026 Market Value
Unverified Web-Scraped Data	\$50 / TB	\$8 / TB (Commoditized/Slop)
Cryptographically Verified Human Telemetry	\$450 / TB	\$2,800+ / TB (Premium)

(Source Data: Enterprise AI Training Set Market Pricing, Q3 2026)

In this zero-trust environment, legacy digital identity is obsolete. The market requires irrefutable, cryptographic proof of human provenance, making Digital Sovereignty an urgent economic necessity for enterprises and insurers. Open and closed, large, small, and local learning models must know if the data they ingest is anchored to a verified, sovereign human, or if it is merely malicious algorithmic noise.

2.3 Life by IDIA: Individual Sovereign Node Architecture & Operational Status

Operating Status: Production (Live on iOS App Store, v1.0.5)

Life by IDIA functions as the primary client-side interface and Sovereign Node for individual contributors within the IDIA ecosystem. The application is deployed in production on iOS, serving as a non-custodial digital asset manager, edge-level data consent gateway, and personal telemetry repository.

Functional Layer	Production Status & Technical Capabilities
Non-Custodial Multi-Asset Sovereign Wallet	Live: Base L2 wallet supporting USDC, IDIA Governance Token, native ETH (gas), and Synapse Credit ledger tracking.
On-Chain Governance Gateway (Wyoming DUNA Interface)	Live: Integrated voting power delegation via OpenZeppelin ERC20Votes contract calls and <code>syncGovernanceState</code> event monitoring.
Edge Consent & Data Lineage Manager	Live: Granular, purpose-specific consent toggles establishing Auditable Consent Artifacts (ACAs) before data packaging.
Bio-Telemetry & Mobility Diagnostics (CPM)	Live (Pro Tier): Gait tracking, cadence, walking asymmetry, and step volume trends via native iOS HealthKit device bridges.
Decentralized Community Grant Pool Monitoring	Live: Monitoring interface for the 10% jurisdictional fee allocation pool.



Production Core Capabilities:

- **Multi-Rail Sovereign Wallet:** Facilitates local key generation and non-custodial asset custody on the Base network, displaying live balances for USDC, IDIA Governance Tokens, network gas, and internal Synapse Credits.
- **Base L2 Governance Integration:** Features direct contract interactions with `IDIAGovernor.sol` and `IDIAEscrow.sol`, allowing token holders to view active voting weight, execute self-delegation, or delegate governance authority to community representatives on-chain.
- **Consent Management & PII Stripping:** Enforces edge-level data hygiene by maintaining local permission registries. Direct identifiers are cryptographically decoupled from local sensor streams prior to transmission or batch staging.
- **Cognitive Performance Module (CPM) Telemetry:** Implements baseline passive mobility diagnostics (walking speed in km/h, asymmetry percentage, daily activity volume) to compute initial biological uptime and operational readiness indices.

Phased & Roadmap Capabilities:

- **Life Pro+ & Pure Alpha Advanced Diagnostics:** Advanced clinical biosensor ingestion, deep heart-rate variability (HRV) continuous correlation, and automated cross-context fatigue alerts are currently in closed beta testing.
- **Decentralized Offline NFC Tap-to-Earn:** Peer-to-peer data verification handoffs via near-field communication remain synchronized with the upcoming pilot merchant rollout.

The Life Pro Series (Tiered Instrumentality & Operational Readiness): Further verification and human optimization are executed through the *Life Pro Series*—comprising **Pro**, **Pro+**, and **Pure Alpha**. Each tier features liveliness reliability engines designed to guide the Sovereign Node in enhancing their own human instrumentality goals, powered by the centralized bio-telemetry codex known as the **Human Reliability Index (HRI)**, which measures Biological Uptime metrics such as sleep architecture, Heart Rate Variability (HRV), and cognitive reaction:

- **Life Pro (\$9.99/month — The Gig & Workforce Standard):** Features the **Cognitive Performance Module (CPM)**, utilizing native mobility and biometric bridges to assess baseline biological readiness and physical uptime for the everyday workforce and gig-economy class.
- **Life Pro+ (\$49.99/month — High-Consequence Occupational Readiness):** Combines the **CPM** with the **Occupational Performance Module (OPM)** to contextualize readiness metrics for specific high-risk, high-consequence roles—such as commercial



pilots, surgeons, logistics fleet operators, and professional athletes—complete with real-time readiness alerts and instrumentality tooling.

- **Pure Alpha (\$99.99/month — Executive & Commercial Synthesis):** Integrates both the **CPM** and **OPM** directly with the financial and operational models of the user's **IDIA Pay** business node, delivering executive-level operational insights that correlate commercial performance with physical and cognitive health (*advanced clinical-grade biosensors and continuous cross-context fatigue alerts currently in closed beta testing*).

2.4 IDIA Pay: Business Sovereign Node Architecture & Pilot Development Status

Operating Status: In Active Development / Pilot Staging (Targeted Louisville Launch)

IDIA Pay serves as the commercial operating system and Business Sovereign Node within the IDIA ecosystem, engineered to capture real-time merchant transaction velocity and operational telemetry. Unlike *Life by IDIA* (which is deployed in production on iOS), *IDIA Pay* is in active development and staging, serving as the core infrastructure vehicle for the upcoming Louisville, Kentucky commercial pilot.

Component Module	Technical Capability & Development Status
Web POS Interface (Point-of-Sale)	Staged: Cloud-based Point-of-Sale terminal supporting multi-category menus, order routing, and ticket reconciliation.
Warehouse Management (WMS) & Inventory Engine	Staged: Smart catalog tracking receiving, put-away, lot/serial expiration, and supply-chain variance logging.
Business Health Index (BHI) Diagnostic Layer	Staged: Algorithmic scoring engine measuring operational velocity, margin stability, and commercial health metrics.
NFC SoftPOS Tap-to-Pay & Local Settlement Rails	In Development: Hardware-free payment rail undergoing native mobile bridge testing and payment facilitator certification.
Fiat Money Transmission & FBO Banking Rails	Pending Regulatory Execution: Direct fiat operations gated behind Phase 1 State MTL applications (CA, TX, NY, FL) & partners.

- **Vertical SaaS Terminal & WMS:** Delivers an integrated merchant dashboard managing catalog inventory, purchase orders, operational shrinkage detection, and transaction logging.
- **Business Health Index (BHI):** Ingests anonymized operational data to model commercial viability and predictive inventory requirements, generating the core operational telemetry streams licensed across *The IDIA Hub*.



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

- **Hybrid Settlement Architecture:** Designed to support dual-rail payment processing—featuring 0% processing fees for closed-loop IDIA-USD/stablecoin transactions and competitive market-rate processing (2.5% + \$0.10) for legacy card networks.

Development & Regulatory Dependencies:

- **Money Transmitter Licensing (MTL) & Banking Integration:** Direct fiat custodial operations and Automated Clearing House (ACH) instant off-ramps operate in partnership with licensed financial institutions, with direct transmission authority phased alongside IDIA's multi-state MTL roadmap.
- **Pilot Merchant Cohort:** Full commercial validation is scheduled through a controlled rollout of 10 to 15 paid Founding Partner merchants in Louisville, validating point-of-sale stability and data ingestion prior to national market expansion.

2.5 The IDIA Hub: Enterprise Data Marketplace & Licensing Desk Architecture

Operating Status: Production Web Application Beta (hub.thebigidia.com)

The IDIA Hub is the enterprise execution terminal, data marketplace, and commercial licensing desk for the IDIA ecosystem. It provides quantitative analysts, institutional algorithms, and autonomous AI agents with low-latency access to cryptographically validated, zero-PII data feeds.

Production Module	Demonstrable Technical Workflow
Data Marketplace Catalog & Curated Bundles	Live: Interactive browsing across NAICS/GICS sectors, lifestyle clusters, and point-of-sale aggregates.
Vulture Ingestion & Sanitization Pipeline	Live: Ingestion agent pipeline enforcing automated PII stripping, schema scrubbing, and privacy-safe ledger logging.
Trading Desk & API Key Management	Live: Self-service credential provisioning, granular scope bounding, rate monitoring, and low-latency endpoint documentation.
Model Context Protocol (MCP) Bridge & Edge Relay	Live: Standardized MCP tool schemas and streaming socket connections enabling autonomous AI agent context injection.
Synapse Credit Billing & Gas Metering	Live: (Base USDC/Crypto) with dynamic gas metering (0.1 to 1.0 credits per query call).



Demonstrable Production Capabilities:

- **Interactive Data Marketplace & SQL Viewer:** Enterprise buyers can browse pre-packaged sector bundles or construct parameterized queries across behavioral and operational taxonomies, viewing live sanitized extracts directly in the platform.
- **The Vulture Sanitization Pipeline:** Demonstrates automated data processing that strips direct identifiers, isolates PII at the boundary, and generates audit hashes certifying compliance before datasets become accessible.
- **Developer Trading Desk & Feature Feeds:** Allows enterprise users to generate production API credentials, configure rate limits, and query REST and WebSocket endpoints supporting low-latency data consumption.
- **Model Context Protocol (MCP) Agent Interface:** Demonstrates direct, two-way integration with autonomous AI frameworks via the IDIA MCP Bridge, exposing standardized tools and telemetry resources for agentic consumption.
- **Synapse Credit Metering & Dual Settlement:** Demonstrates instant balance funding via credit card or Web3 wallet connection, with real-time credit deduction as data payloads are requested and delivered.

Demonstrable End-to-End Enterprise Licensing Workflow:

1. **Authentication & Vault Provisioning:** The enterprise buyer registers an organizational account on hub.thebigidia.com and provisions an operational vault.
2. **Treasury Funding:** The buyer deposits funds via fiat or USDC, minting an active balance of virtual Synapse Credits within their billing profile.
3. **Query Construction or Stream Binding:** The buyer selects a target data bundle or connects their autonomous agent via the MCP socket bridge.
4. **Boundary Verification & Settlement Execution:** The Synapse Engine validates credit reserves, verifies ACA permissions and boundary compliance (utilizing The Vulture pipeline where third-party enterprise datasets are ingested), and returns the payload while logging the consumption event to the settlement ledger.

2.6 Protocol System Architecture & End-to-End Data Pipeline

The IDIA Protocol operates as a vertically integrated pipeline comprising five distinct layers:

Edge Ingestion, Consent & Sanitization, Core Analytical Orchestration, Enterprise Licensing, and Settlement & Settlement Governance.



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

Architectural Layer	System Components & Technical Functions
LAYER 1: CLIENT APPLICATIONS & TELEMETRY SOURCES (THE EDGE)	Life by IDIA (iOS/Android): Bio-Telemetry (CPM), Mobility & Gait Trends, Non-Custodial Wallet. IDIA Pay (Web POS / V-SaaS): Point-of-Sale Data, WMS Inventory Variance, Merchant Cash Flows. Home & Spatial Nodes (IoE): Environmental State, Power/Energy Telemetry, Local Edge Diagnostics.
LAYER 2: CONSENT, PROVENANCE & SANITIZATION LAYER	• Auditable Consent Artifacts (ACA): SHA-256 Hashing and Zero-Knowledge generation. • Client-Side PII Decoupling: Hardware Keystore and Local Enclave Isolation. • The Vulture Pipeline: Ingestion Schema Normalization & Differential Privacy Scrub. • Crazy Friend AI: Edge Injection Defense & Real-Time Boundary Verification.
LAYER 3: CORE ANALYTICS & ROUTING (THE IDIA SYNAPSE ENGINE)	• Valuation Engine: Synapse Gas & Credit Pricing Calibration. • Diagnostic Codex: Human Reliability Index (HRI) & Business Health Index (BHI). • LangGraph Orchestrator: Multi-Agent State Verification & Feature Assembly. • Secure Storage: AWS GovCloud / Commercial Cloud (PostgreSQL RLS & S3 Data Lake).
LAYER 4: ENTERPRISE DATA MARKETPLACE & LICENSING (THE IDIA HUB)	• Execution Terminal: hub.thebigidia.com Data Marketplace Catalog. • Delivery Channels: Ultra-Low Latency Feature Feeds ($\leq 100\text{ms}$ SLA), Model Context Protocol (MCP) Bridge, Parameterized SQL Marketplace. • Client Profiles: Quant Desks, Enterprise AI Developers, Insurers, Public Infrastructure.
LAYER 5: CLEARING, ROYALTIES & FINANCIAL SETTLEMENT	Trigger: Synapse Credit Consumption Event (\$0.75 / Credit). Programmatic Revenue Split: • 60% Platform Operations & Infrastructure Reserve (IDIA Data Inc.). • 30% Contributor Royalty Pool (USDC Settlement). • 10% Localized Treasury / Regional Grant Pool (IDIA_LocalizedPool.sol). On-Chain Anchoring (Base L2): • IDIALiabilityReceipt.sol (Soulbound ERC-721 Data Purchase NFT). • 1:1 IDIA Governance Token Distribution via Escrow. • IDIAGovernor.sol & TimelockController DAO Governance. • IDIA Indemnity Reserve, LLC: Series I Telemetry (\$SITs) Variable Sweep (\$0.25).



Architectural Layer Descriptions

1. **Client Ingestion Nodes (The Edge):** Captures multi-modal telemetry across individual contributors (*Life by IDIA*), commercial merchants (*IDIA Pay*), and environmental sensor perimeters. Raw data remains strictly localized on the host hardware or non-custodial secure storage.
2. **Consent & Sanitization Gate:** Every payload is bound to an immutable Auditable Consent Artifact (ACA) generated at the device level. Direct identifiers are irreversibly decoupled at the device edge via local hardware enclave isolation and verified at the boundary by Crazy Friend AI and the Crazy 8 security suite (while third-party enterprise datasets are sanitized via The Vulture pipeline), ensuring zero PII enters the processing core, while autonomous *Crazy Friend AI* agents prevent malicious injection attacks.
3. **The IDIA Synapse Engine:** Operates as the central routing, diagnostic, and valuation layer. It normalizes heterogeneous telemetry streams into standard analytical outputs—including the Human Reliability Index (HRI) for operational readiness and the Business Health Index (BHI) for commercial vitality—and prices consumption dynamically.
4. **The IDIA Hub Licensing Desk:** The enterprise procurement interface (`hub.thebigidia.com`), serving institutional buyers via low-latency feature feeds ($\leq 100\text{ms}$ SLA), standardized Model Context Protocol (MCP) tool endpoints for autonomous AI agents, and secure SQL extract catalogs.
5. **Clearing & Settlement Rails:** When an enterprise consumes Synapse Credits, the protocol executes an automated financial split: 60% covers Platform Infrastructure (IDIA Data Inc.), 30% is directed to the Contributor Royalty Split in USDC, and 10% funds localized regional community grant pools. Concurrently, a soulbound IDIALiabilityReceipt NFT is minted to the buyer on Base L2, while matching IDIA Governance Tokens are routed to contributors to guarantee participatory network ownership." (Note: Also change "30% Contributor Royalty Pool (USDC Settlement)" inside the Layer 5 table just above it to "30% Contributor Royalty Split (USDC Settlement)").

2.7 Systems Maturity Matrix: Production Systems vs. Roadmap Architecture

To maintain institutional compliance and complete transparency during technical due diligence, IDIA Data Inc. explicitly demarcates operational systems deployed in production from staged pilot modules, pending integrations, and forward-looking roadmap initiatives.



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

Lifecycle Tier	System / Component	Current Operational & Deployment Status
TIER 1: PRODUCTION (Live Operational Software)	Life by IDIA (Consumer Node)	Deployed live on Apple iOS App Store (v1.0.5); supports non-custodial multi-currency wallet, edge consent toggles, and base CPM mobility tracking.
	The IDIA Hub Beta (Enterprise Desk)	Live production web application (hub.thebigidia.com) featuring catalog browsing, Vulture sanitization, API credentialing, and Synapse Credit billing.
	Base L2 Smart Contracts	Deployed on Base Mainnet (0x6526...01FB); live Uniswap liquidity, IDIA Governor, IDIA Escrow vaults, and soulbound IDIA Liability Receipt minting rails.
TIER 2: PILOT STAGING (Functional MVP / Closed Testing)	IDIA Pay POS & WMS (Merchant Node)	Functional MVP staged for Louisville pilot; cloud POS catalog, inventory shrinkage detection, and core Business Health Index (BHI) scoring engine.
	Founding Partner Network	Pilot operational framework established for 10–15 paid commercial merchants in Louisville, KY.
TIER 3: PLANNED INTEGRATIONS (In Development / Regulatory Gated)	NFC SoftPOS Tap-to-Pay	In active mobile-bridge development; hardware-free tap-to-pay awaiting final acquirer certification.
	Fiat Transmission & FBO Banking	Gated behind Phase 1 State Money Transmitter Licenses (CA, TX, NY, FL) and partner bank APIs.
	Advanced Biosensors (HRI Diagnostic)	Life Pro+ and Pure Alpha continuous HRV and stress telemetry engines undergoing internal beta testing.
TIER 4: FUTURE ROADMAP (Post-Series A Initiatives)	Angelic XR Dedicated Hardware / Glass	Spatial computing PaaS and proprietary commercial AR eyewear engineered for tourism and MICE.
	Sovereign GovCloud	Firewalled AWS GovCloud enclave architecture for FAR-compliant federal agency procurement (NIH/DOD).



Operational Verification Criteria:

1. **Tier 1 (Production Systems):** Supported by live codebase repositories, active public network smart contracts, and verifiable end-user client installations.
2. **Tier 2 (Pilot Staging):** Fully functional codebases operating in restricted environments, ready for scheduled localized merchant and user deployment.
3. **Tier 3 (Planned Integrations):** Systems requiring external regulatory capital (e.g., state licensing surety bonds) or partner bank API integration before broad consumer distribution.
4. **Tier 4 (Future Roadmap):** Strategic scaling architectures requiring Series A capitalization and dedicated corporate development or hardware supply chain execution.

IDIA Protocol Summation

Life by IDIA and IDIA Pay capture data from Sovereign Nodes, while The IDIA Hub is the data marketplace, where captured data can be purchased by MCP servers, API endpoints, SQL, raw AI al a carte and curated data bundles, and our data marketplace AI in-house chatbot Best Friend AI. The Synapse Engine powers the Protocol, ensuring all captured data is tagged, staged, rated and priced, along with routing the data royalty payout procedure and synapse gas consumption weighting.

All Sovereign Nodes are verified with the Life by IDIA app before access to the rest of the IDIA Protocol, this is a mandatory requirement that Verifies liveliness reliability, through liveliness checks via data consumption and biometric challenges. When Sovereign Nodes provide Data, the Synapse Engine routes Data Royalty from Synapse Credit consumption occurring from The IDIA Hub, which ensures that as AI Agents require "Ground Truth" to function safely, humans can monetize their proven reliability—the one thing AI cannot forge. Data Yield is paid out instantaneously in **USDC stablecoin** on the Base Layer-2 network, matched 1:1 numerically with the **IDIA Governance Token**.

Why the Agentic World Needs This to Survive

The rise of "Agentic Commerce" (AI Agents buying/selling autonomously) faces two existential threats: Model Collapse and Litigation Extinction. Without a source of "Ground Truth," AI models trained on synthetic data degrade into hallucination (Model Collapse). Furthermore, if an Agent executes a bad trade or a negligent action based on hallucinated data, the developer faces uncapped liability lawsuits.

IDIA is the verification layer for the agentic economy. The Synapse Engine provides ground truth APIs and web hooks that prevents collapse. More importantly, the IDIA Liability Shield wraps



every data packet in a Liability Token, a sole-bound NFT. This token acts as "Litigation Armor" for the AI Agent. If the Agent acts on IDIA data, it can cryptographically prove that its decision was based on Verified Truth, shifting liability away from the algorithm. Without this "Verification Shield," the Agentic economy will be sued into oblivion.

2.8 Third-Party Hardware Dependencies & Operational Boundaries

To accurately scope platform liability, technical execution, and privacy enforcement, IDIA explicitly defines the demarcation line between its proprietary protocol layer and the third-party Original Equipment Manufacturer (OEM) hardware dependencies that remain strictly outside IDIA's control.

1. Biometric & Telemetry Sensors (Apple HealthKit / Google Fit)

- **The Dependency:** *Life by IDIA* and the Cognitive Performance Module (CPM) rely entirely on native OS bridges (e.g., Apple HealthKit, Google Fit) and third-party wearables (e.g., Apple Watch) for raw physiological and mobility data ingestion.
- **The Operational Boundary:** IDIA does not control sensor accuracy, hardware calibration, or physiological capture mechanics. If a third-party wearable records anomalous biometric data, the IDIA pipeline ingests it as presented. Furthermore, background data polling is strictly governed by native iOS/Android battery management and privacy throttling; IDIA cannot force continuous background extraction beyond OEM limits.

2. Cryptographic Storage & Edge Isolation (Secure Enclave / Keystore)

- **The Dependency:** Non-custodial wallet key generation, Auditable Consent Artifact (ACA) hashing, and local PII isolation rely on the host device's native hardware security modules (Apple Secure Enclave, Android Keystore).
- **The Operational Boundary:** IDIA's security architecture assumes the integrity of the underlying OEM hardware. The protocol cannot prevent data compromise resulting from root-level OS vulnerabilities, device jailbreaking, or OEM firmware exploits that compromise the device's fundamental secure storage capabilities.

3. SoftPOS Payments (NFC Modules)

- **The Dependency:** The *IDIA Pay* NFC Tap-to-Pay architecture relies on native device Near-Field Communication (NFC) controllers and payment facilitator SDKs (e.g., Apple Tap to Pay, Android Host Card Emulation).



-
- **The Operational Boundary:** IDIA cannot override native NFC hardware failures, OS-level NFC access restrictions, or baseband processor latency that may temporarily disrupt hardware-free payment processing at the point of sale.

4. Spatial & Environmental Telemetry (ARKit / ARCore / Smart IoT)

- **The Dependency:** Spatial data captured for *Angelic XR* and environmental telemetry captured by Home Nodes rely on Apple ARKit, Google ARCore, and third-party smart appliance APIs (IoE).
- **The Operational Boundary:** IDIA is subject to the API rate limits, firmware updates, and deprecation schedules of these external smart home and spatial computing ecosystems. Disputed sensor measurements from third-party hardware are flagged by the IDIA Synapse Engine's diagnostic layer, but IDIA cannot independently recalibrate the external hardware source.

2.9 Integration Dependencies & Operational Fallback Protocols

To ensure continuous operation of the *Verified Truth Economy*, IDIA maintains a comprehensive Site Reliability Engineering (SRE) posture. The protocol mitigates external vendor lock-in and Single Points of Failure (SPOFs) through dynamic routing, asynchronous queueing, and redundant fallbacks.

1. Cloud Infrastructure & Data Storage (AWS)

- **The Dependency:** The IDIA Synapse Engine, Vulture Pipeline, and Hub data lake operate on Amazon Web Services (AWS/GovCloud), utilizing RDS for structured state and S3 for sanitized data warehousing.
- **SPOF Risk:** A localized AWS availability zone (AZ) or regional cloud outage.
- **Operational Fallback:** The microservices architecture utilizes Amazon SQS (Simple Queue Service) and Step Functions to decouple data ingestion from processing. In the event of an RDS or regional outage, incoming telemetry is durably cached in decentralized edge queues or multi-region S3 buckets, preventing data loss until analytical processing can safely resume.

2. Fiat Processing & Money Transmission Gateways (Pending)

- **The Dependency:** Fiat on/off-ramps and legacy card processing for *IDIA Pay* and *The IDIA Hub* rely on external payment facilitators and acquiring banks (e.g., Fiserv, Worldpay, Coinbase).
- **SPOF Risk:** Gateway downtime, API rate limiting, or acquiring bank network failure.

- **Operational Fallback:** The platform employs multi-gateway AI routing. If the primary fiat processor experiences downtime, transactions are automatically rerouted to secondary merchant acquirers. Furthermore, closed-loop transactions utilizing IDIA-USD stablecoins bypass external fiat rails entirely, ensuring internal ecosystem commerce remains uninterrupted.

3. Base L2 Blockchain & RPC Endpoints

- **The Dependency:** Immutable ledger logging, IDIALiabilityReceipt NFT minting, and DAO governance transactions execute on the Base Layer-2 network.
- **SPOF Risk:** Base sequencer downtime or failure of the primary Remote Procedure Call (RPC) node provider (e.g., Alchemy, Infura).
- **Operational Fallback:** IDIA maintains a multi-provider RPC rotation. If a provider fails, traffic shifts instantly to backups. If the underlying Base network experiences a sequencer halt, the IDIA Synapse Engine places settlement transactions into an asynchronous queue. Edge devices continue to operate via local caching, and queued state changes are batch-settled once Layer-2 finality is restored.

4. AI Inference & Multi-Agent Orchestration

- **The Dependency:** The LangGraph orchestrator and *Crazy Friend AI* agents rely on external foundation models (e.g., OpenAI, Anthropic, Gemini) for complex schema inference and NLP parsing.
- **SPOF Risk:** API throttling, token limit exhaustion, or foundation model service degradation.
- **Operational Fallback:** The LangGraph framework is explicitly model-agnostic. The system continuously monitors API latency and can dynamically failover from a primary foundation model to a secondary provider without interrupting the Vulture sanitization pipeline or the enterprise Model Context Protocol (MCP) endpoints.

2.10 IDIA Home Nodes: Residential Properties as Operating Systems

Operating Status: Architectural & Edge-IoE Integration Framework

Beyond individual wearables (*Life by IDIA*) and merchant terminals (*IDIA Pay*), the IDIA Protocol reclassifies residential properties from "Passive Collateral" into active **Home Nodes**. Within the IDIA ecosystem, a home functions as an anonymized, sensor-rich operating environment. From smart televisions and appliances to lighting grids and HVAC systems,



ambient environmental state and power consumption are captured in real time and anonymously to validate energy utilization, environmental telemetry, and human presence ("Proof of Life").

1. External Enterprise Yield Generation

The data yield generated by a Home Node is derived strictly from commercial licensing sales to external enterprise clients—including Utility Grids, Logistics Networks, and Insurance Carriers—via *The IDIA Hub*. Provisioned via sovereign capital, the Home Node offsets its own carrying costs through exported, cryptographically verified environmental truth.

2. Occupancy as Revenue: The Market-Driven Aid Against Houselessness

The Home Node architecture fundamentally alters the unit economics of residential real estate. Under the legacy Mortgage-Backed Standard, a vacant investment property passively appreciates in value, incentivizing institutional hoarding and exacerbating houselessness. Within the IDIA Protocol, a Home Node only generates data yield if a verified Human Operator resides inside to generate continuous "Proof of Life" and consumption telemetry.

- An unoccupied property generates **\$0.00** in data yield.
- This inverts the landlord incentive structure: property owners are economically incentivized to place human occupants into residential units—even at heavily subsidized or zero rent—solely to activate the environmental data stream and unlock the asset's commercial telemetry yield. By making human occupancy a prerequisite for asset performance, the protocol utilizes market forces to turn shelter from a passive debt obligation into a productive input for the Verified Truth Economy.

3. Edge Computing, Zero-Knowledge Proofs (ZKPs), and the PII-Free Database Doctrine

To eliminate the risk of centralized domestic surveillance, the Home Node is governed by strict edge-processing and cryptographic isolation:

- **Local Hardware Siloing:** While the Home Node captures hyper-granular telemetry from smart appliances, spatial sensors, and biological operators, personal identity never leaves the premises. All Personally Identifiable Information (PII) is cryptographically siloed on local hardware or stripped prior to staging.
- **Zero-Knowledge Proof (ZKP) Validation:** When external enterprise buyers (such as utility grids or property insurers) require verification of occupancy or energy state, the Home Node employs Zero-Knowledge Proofs (ZKPs). The ZKP computes the verification locally at the edge and transmits only the mathematically validated proof to *The IDIA Hub* from Internet-of-Everything (IoE) devices, completely severing the commercial transaction from the occupant's underlying identity.



Section 3

DATA RIGHTS, ADMINISTRATIVE AGENCY, AND CONSENT

3.1 Data Asset Taxonomy & Lineage Classification

To enforce strict regulatory compliance, minimize liability, and define the exact commercial deliverables administered by the IDIA Protocol, all ecosystem data is systematically classified into five distinct operational tiers:

1. Raw Telemetry (Tier-0 Sovereign Data)

- **Definition:** Unprocessed, direct observational exhaust generated at the hardware edge. This includes raw biological waveforms (e.g., HRV/ECG readings), precise geolocation pings, unstructured IoT sensor logs, and raw Point-of-Sale (POS) ticket data.
- **Status:** Raw Tier-0 telemetry is strictly non-commercial. It is isolated within secure hardware enclaves (e.g., AWS Nitro Enclaves or local device Keychains) and is never transmitted, licensed, or sold to enterprise buyers.

2. Pseudonymized Records

- **Definition:** Edge-processed telemetry that has been permanently stripped of direct identifiers (names, exact addresses, SSNs) and bound to an Auditable Consent Artifact (ACA).
- **Status:** This is the baseline format transmitted to *The IDIA Hub*. While direct identifiers are removed, the data remains mathematically linked to a decentralized identifier (DID) to allow for royalty attribution and consent revocation without revealing the human identity.

3. Derived Metrics

- **Definition:** First-order analytical outputs generated by the IDIA Synapse Engine applying proprietary algorithms to pseudonymized records.
- **Status:** Examples include the Human Reliability Index (HRI) and the Business Health Index (BHI). Derived metrics represent operational status (e.g., commercial margin stability or biological uptime) rather than exposing the underlying raw data that generated the score.



4. Aggregated Datasets

- **Definition:** Macro-level compilations of pseudonymized records and derived metrics grouped by geographic, demographic, or behavioral cohorts (e.g., "Retail Velocity in Zip Code 40216").
- **Status:** Aggregation enforces strict privacy thresholds, ensuring no individual contributor can be reverse-engineered or isolated from the cohort.

5. Licensed Data Assets

- **Definition:** The final commercial deliverable procured by the enterprise buyer. A Licensed Data Asset is a verified, Zero-PII bundle or feature feed (comprising derived metrics or aggregated datasets) that is cryptographically packaged with its originating ACAs and a contractual liability shield.
- **Status:** This is the exclusive data tier that triggers a Synapse Credit consumption event and subsequent royalty distribution.

3.2 Data Rights and the Administrative Agency Model

The IDIA Protocol is designed to help individuals and businesses register eligible data contributions, document applicable permissions, and authorize defined commercial uses of their data assets. It operates strictly under a model of administrative agency and commercial licensing.

Retention of Applicable Rights

Contributors retain the rights they hold in their underlying raw telemetry (Tier-0 Sovereign Data), subject to applicable law and any valid licenses or permissions previously granted. By connecting a data source—such as a wearable device via *Life by IDIA* or a Point-of-Sale terminal via *IDIA Pay*—and providing the required affirmative consent, a contributor authorizes IDIA Data Inc. to administer and license the specified data assets within the strict scope of that authorization.

Limits of Authority & Contractual Boundaries

IDIA's authority is strictly limited to the rights, permissions, and contractual powers it validly receives from the Sovereign Node. Registration on the protocol does not:

1. Establish absolute property ownership over all ambient information or public facts associated with an individual.
2. Confer legal rights over independently collected third-party information operating outside the IDIA ecosystem.



-
3. Guarantee that every unauthorized external use of a person's identity across the broader internet can be prevented or monetized.

IDIA functions exclusively as a commercial licensing agent and technical clearinghouse for the data explicitly submitted, verified, and legally consented to within its protocol.

3.3 Scope of Grant: The Administrative Agency Authorization

When a Sovereign Node connects a data source to the IDIA Protocol (e.g., via *Life by IDIA* or *IDIA Pay*), the contributor executes a specific, limited, and revocable grant of authority. This grant empowers IDIA Data Inc. to act as the administrative licensing agent for that specific telemetry stream, strictly bounded by the following authorized actions:

1. Authority to Ingest, Sanitize, and Strip PII The contributor grants IDIA the technical authority to ingest raw telemetry (Tier-0) from connected devices, normalize the data schema, and permanently decouple Direct Identifiers (PII) to create privacy-safe Pseudonymized Records.

2. Authority to Generate Derived Metrics and Aggregates The contributor authorizes the IDIA Synapse Engine to process their pseudonymized records through proprietary diagnostic algorithms to generate Derived Metrics (such as the Human Reliability Index or Business Health Index) and to compile their data into macro-level Aggregated Datasets.

3. Authority to License and Sublicense (The Hub) Subject to the granular consent toggles actively set by the user, the contributor grants IDIA a non-exclusive, sub-licensable right to commercialize the resulting Licensed Data Assets through *The IDIA Hub*. This includes the authority to present and distribute the data to verified enterprise buyers, autonomous AI agents, and institutional data consumers under IDIA's Master Service Agreements (S-3-C).

4. Authority to Collect and Distribute Royalties The contributor grants IDIA the financial agency to negotiate market clearing prices (via Synapse Credit consumption), collect fiat and digital asset revenues from enterprise buyers on their behalf, and programmatically distribute the owed performance royalties (USDC and IDIA Governance Tokens) to the contributor's designated sovereign wallet.

Strict Limitations on the Scope of Grant This authorization is strictly non-exclusive and revocable. Contributors retain the right to disconnect sources or revoke consent for future commercial licensing at any time. The grant explicitly prohibits IDIA from selling raw, un-sanitized PII, and legally restricts IDIA from exceeding the use-cases authorized by the device-level Auditable Consent Artifact (ACA).

3.4 The Universal Basic Asset (UBA): An Administered Asset Class

IDIA rejects the concept of Universal Basic Income (UBI)—a redistributive handout that risks hyperinflation—in favor of the Universal Basic Asset (UBA). However, within the IDIA Protocol, the UBA operates as a highly defined, **administered asset class**.

The UBA is strictly composed of the localized telemetry that individuals and businesses (Sovereign Nodes) actively capture, verify, and authorize for commercial licensing through IDIA's native interfaces.

Establishing the Sovereign Node & Data Catalog To create, administer, and monetize a UBA, contributors interact with the IDIA ecosystem through specific ingestion nodes rather than claiming sweeping rights over the broader web:

- **Life by IDIA (The Individual Node):** Serves as the primary client interface where users capture localized biological, mobility, and financial telemetry, permanently binding it to granular, purpose-specific consent toggles before it ever leaves the device.
- **IDIA Pay (The Business Node):** Captures verified commercial velocity, point-of-sale transactional flow, and inventory state data from participating merchants.
- **The IDIA Hub (The Marketplace):** Functions as the commercial clearinghouse where this authorized, zero-PII data catalog is sub-licensed to enterprise and algorithmic buyers.

By substituting legally fictitious property claims with enforceable, bilateral commercial licensing, the UBA transitions users from uncompensated subjects of the data economy into active, legally defined participants. The protocol bypasses the burden of proving ownership over public facts by executing a valid administrative license to distribute a verified, secure data feed on the user's behalf, generating a programmatic Data Royalty directly tied to Synapse Credit consumption.

3.4.1 The Fiscal Architecture: The Sovereign Proprietorship

By establishing the Universal Basic Asset (UBA), the IDIA Protocol fundamentally repositions the tax and commercial classification of the individual contributor. Rather than acting as a passive consumer, a participating Sovereign Node operates as a **Sole Proprietor** engaged in commercial data production, subject to applicable tax law and individual professional tax counsel:

1. The Schedule C Standard and the 24/7 Operations Rationale

Under the Sovereign Proprietorship framework, a contributor registering data sources and licensing telemetry for commercial royalties engages in the active trade or business of high-



fidelity data production, categorizing earned Synapse Yields as self-employment/business income (IRS Schedule C). Unlike traditional W-2 wage labor, edge data capture and node maintenance operate continuously (24/7/365). Accordingly, contributors operating qualified business nodes may evaluate applicable **IRC §162 ordinary and necessary business deductions**—such as a pro-rata share of home internet connectivity, ambient electrical utility draw ("Ghost Load"), and qualifying hardware depreciation (**IRC §179**)—required to power and maintain their local data-refining infrastructure.

2. Automated Substantiation via the Pattern of Life (PoL) Ledger (IRC §6001)

To satisfy statutory substantiation requirements under **IRC §6001**, *Life by IDIA* includes the automated **Pattern of Life (PoL) Ledger**. The PoL Ledger logs every kilobyte of telemetry licensed, every Auditable Consent Artifact (ACA) executed, and the corresponding device uptime and power telemetry, generating immutable, audit-ready substantiation records for the contributor's tax filings.

3.5 Jurisdictional Boundaries and Third-Party Data Isolation

Registration on the IDIA Protocol establishes a legally bounded administrative relationship. The protocol exerts administrative and commercial licensing authority strictly over the telemetry actively captured, verified, and consented to within native IDIA applications, including *Life by IDIA* and *IDIA Pay*.

Exclusion of Independent Third-Party Observations

The IDIA Protocol operates independently of external data brokers, social networks, and legacy digital ecosystems. The execution of a user registration agreement confers zero authority, ownership, or enforcement capability to IDIA regarding data collected independently by third parties operating outside the IDIA network.

Limitation of Enforcement Liability

IDIA functions exclusively as the administrative agent for its internal data marketplace. The company possesses no legal mandate, operational capability, or fiduciary obligation to monitor, police, or monetize a contributor's identity across the broader internet. Liability, regulatory compliance, and royalty generation are mathematically and legally confined to the zero-PII data explicitly processed via the Synapse Engine and distributed via *The IDIA Hub*.

3.6 The Lifecycle of the Auditable Consent Artifact (ACA)

To guarantee that the administrative agency model remains structurally sound, the IDIA Protocol treats consent as a dynamic, cryptographic lifecycle rather than a static legal agreement. The



Auditable Consent Artifact (ACA) governs this lifecycle through four distinct operational phases:

Creation at the Edge

When a Sovereign Node enables a specific telemetry stream (e.g., granting mobility tracking in *Life by IDIA* or inventory logging in *IDIA Pay*), the client application generates a time-stamped cryptographic hash (SHA-256) representing the exact permission parameters. This ACA is generated locally on the device, permanently binding the authorization logic to the outbound data payload before it is transmitted.

Real-Time Verification

Before any incoming payload is accepted into the protocol's core analytical routing, the IDIA Synapse Engine and *Crazy Friend AI* edge-defense agents independently verify the attached ACA signature and strips any PII. If a payload arrives with an invalid, expired, or missing ACA—or if the data type exceeds the bounds of the cryptographic signature—the ingestion is instantly rejected at the perimeter.

Dynamic Updating and Revocation

Consent within the IDIA ecosystem is explicitly non-perpetual and highly dynamic. Contributors can update, narrow, or entirely revoke their permissions at any time via their native application dashboard. Modifying a permission toggle triggers an immediate state-change event, generating a newly hashed ACA for all future telemetry while instantaneously halting the commercial routing of any revoked data streams to *The IDIA Hub*.

Immutable Enterprise Auditing

The metadata of the ACA travels synchronously with the licensed data asset to the enterprise buyer. If an enterprise data consumer faces a regulatory inquiry or compliance audit, they can produce the ACA metadata to mathematically prove the exact time, scope, and active validity of the contributor's consent at the moment of ingestion. This audit capability operates via Zero-Knowledge principles, allowing regulators to verify the chain of custody without ever exposing the underlying raw identifiers of the contributing node.

3.7 Assignment of Claims and Limited Power of Attorney

To effectively administer the commercial licensing of registered data assets and protect the integrity of the ecosystem, contributors grant IDIA Data Inc. a Limited Power of Attorney (LPOA) and a specific assignment of enforcement claims. This legal mechanism is strictly bounded and subject to applicable jurisdictional law.



Scope of the Limited Power of Attorney

Upon affirmative registration of a data source, the Sovereign Node grants IDIA the specific legal standing to:

- Negotiate, execute, and administer Master Service Agreements and Data Processing Addendums with enterprise buyers on the contributor's behalf.
- Collect financial remuneration (fiat and digital assets) resulting from the authorized consumption of the contributor's licensed data assets.
- Enforce the contractual terms of the enterprise license, including pursuing liquidated damages or breach of contract claims against any enterprise buyer that violates the scope of their license (e.g., unauthorized sub-licensing, failure to delete data, or attempting re-identification).

Strict Limits on Enforcement Liability

This Limited Power of Attorney does not constitute a general legal representation or a universal assignment of the contributor's privacy rights. The legal standing is confined exclusively to the enforcement of the bilateral contracts executed within *The IDIA Hub*. IDIA assumes zero fiduciary obligation or legal authority to pursue external third parties, independent data brokers, or external bad actors for general privacy violations, web scraping, or data breaches occurring outside the IDIA Protocol infrastructure. The assignment of claims is solely a commercial mechanism to ensure IDIA can legally deliver, bill, and protect the specific datasets it licenses to verified enterprise consumers.

3.8 Disputed Provenance, Joint Data, and Unauthorized Submissions

To finalize the administrative agency framework and protect the integrity of the enterprise liability shield, the IDIA Protocol enforces strict procedural safeguards to manage complex provenance scenarios, unauthorized submissions, and contested data rights.

Age Restrictions and Protection of Minors

The IDIA ecosystem strictly prohibits the ingestion, processing, or commercial licensing of telemetry generated by minors. Identity verification and Infinite Authentication mechanisms within *Life by IDIA* ensure that only individuals of legal majority age can establish a Sovereign Node and generate an Auditable Consent Artifact (ACA). The protocol does not authorize the processing of any data subject to the Children's Online Privacy Protection Act (COPPA) or equivalent global youth privacy frameworks.



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

Contributor Warranties and Unauthorized Submissions

Upon connecting a data source, the contributor executes a legal warranty affirming they possess the absolute right and authority to license the submitted telemetry. The protocol explicitly prohibits the submission of third-party data without verified consent (for example, an employer attempting to capture and monetize employee telemetry without individual, cryptographic opt-in). If the *Crazy Friend AI* security network or the Vulture pipeline detects anomalous ingestion patterns indicative of unauthorized third-party scraping, the protocol automatically severs the ingestion connection and purges the payload.

Joint and Shared Environmental Telemetry

In contexts where data is generated within shared spaces (such as a Home Node capturing spatial environmental state or IoT telemetry), the registered account holder of the device assumes data responsibility for all occupants, whether temporary guests or permanent residents.

Cryptographic Proof of Authorization

Because it is technically impossible for telemetry to enter *The IDIA Hub* or be available for sale without a mathematically bound ACA, traditional manual data quarantines for "unauthorized submissions" are obsolete. Should an external party contest the commercial right to a dataset, IDIA simply produces the ACA. This provides absolute, immutable cryptographic proof that the data was legally authorized by a verified Sovereign Node prior to any Synapse Credit consumption or enterprise licensing.



Section 4

DATA PRIVACY, SECURITY & RE-IDENTIFICATION

4.1 Data Privacy States: Identification, Pseudonymization, and Aggregation

To ensure enterprise buyers understand the exact regulatory profile of the Licensed Data Assets they procure, the IDIA Protocol enforces a strict taxonomic distinction between various states of data privacy. The protocol explicitly defines and isolates these states across the ingestion and commercial pipelines.

Direct Identification (PII)

- **Definition:** Telemetry or records containing overt markers that explicitly identify a specific human operator or legal entity (for example, legal names, social security numbers, direct contact information, or raw biometric templates).
- **Protocol Handling:** The IDIA Protocol explicitly prohibits the commercial sale, transmission, or enterprise licensing of Direct Identification data. Such markers are either isolated in local hardware keystores at the edge or immediately purged by the Synapse Engine prior to entering the commercial marketplace.

Pseudonymization (Zero-PII)

- **Definition:** The state of data where direct identifiers have been permanently removed and replaced with a deterministic cryptographic hash (e.g., a `pseudo_user_id` generated via SHA-256 and proprietary salts).
- **Protocol Handling:** This is the standard operational state of telemetry within *The IDIA Hub*. Pseudonymization mathematically decouples the data payload from the human identity, protecting the contributor from enterprise exposure while allowing the IDIA Synapse Engine to accurately route performance royalties back to the originating Sovereign Node ledger. The enterprise buyer receives the analytical value of the data without ever possessing the underlying identity.

Aggregation

- **Definition:** The macro-level compilation of pseudonymized records grouped into geographic, temporal, or behavioral cohorts (for example, "average point-of-sale velocity in the 40216 zip code over 30 days").
- **Protocol Handling:** Aggregation dilutes individual data points into statistical trends, providing an additional layer of mathematical privacy. This format is utilized for broad

market-intelligence bundles and public-sector spatial planning, ensuring no single contributor can be isolated from the cohort.

Anonymization

- **Definition:** The absolute, irreversible destruction of all individual traceability, rendering it mathematically impossible to link a data point back to a specific individual, even through advanced inference.
- **Protocol Handling:** Because temporal timestamps, location traces, and highly specific behavioral patterns can theoretically enable re-identification when cross-referenced with massive external datasets, IDIA operates with extreme technical precision. The protocol classifies its commercial deliverables as "Pseudonymized and Zero-PII" rather than claiming absolute "Anonymization," thereby maintaining accurate regulatory alignment and shielding enterprise buyers from over-broad privacy promises.

4.2 Re-Identification Risks and the Mosaic Effect

While the IDIA Protocol enforces rigorous pseudonymization and Zero-PII standards at the ingestion boundary, the platform formally recognizes that the complete elimination of re-identification risk is technically unfeasible in high-fidelity data environments. Removing direct identifiers (such as names or account numbers) does not completely erase the digital shadow of the Sovereign Node.

To maintain complete transparency with enterprise buyers and regulatory bodies, IDIA classifies the following telemetry vectors as inherent re-identification risks:

1. Temporal and Spatial Traces

Continuous location data and precise timestamps act as a highly unique signature. A dataset showing a device traveling from a specific residential coordinate to a specific commercial office building every weekday at 8:00 AM can reliably identify the individual, even if all direct identifying text is stripped.

2. Behavioral and Biological Fingerprinting

The telemetry captured by the Cognitive Performance Module (CPM), including specific gait cadence, walking asymmetry, and highly unique Heart Rate Variability (HRV) baselines, can function as secondary biometric identifiers. When analyzed over extended periods, these behavioral patterns become as statistically unique as a physical fingerprint.



3. Linked Datasets (The Mosaic Effect)

The most severe risk occurs when an enterprise buyer attempts to merge authorized IDIA data with unauthorized, external datasets (such as scraped public records or leaked marketing databases). Through correlation, a buyer could theoretically reconstruct a contributor identity by overlapping disparate data points.

4. Protocol Mitigation and Contractual Prohibition

To address the risks intrinsic to all high-value data, the IDIA Protocol deploys a comprehensive dual-layered defense. Technically, the Synapse Engine and Crazy Shield (the dedicated Data Loss Prevention agent within the Crazy 8 security suite) apply differential privacy techniques, such as spatial fuzzing and timestamp rounding, to dilute unique signatures before the data enters The IDIA Hub. Legally, every enterprise buyer executing a Master Service Agreement commits to a strict, punitive contractual mandate prohibiting any attempt to re-identify, correlate, or reverse-engineer the identity of any IDIA contributor.

4.3 Data Minimization, Access Controls, and Identifier Separation

To mitigate systemic risk and ensure compliance with global privacy frameworks, the IDIA Protocol implements a strict defensive data architecture. The platform operates under the principle that data is a highly regulated utility, requiring precise minimization, rigid access gating, and absolute identifier separation.

1. Mathematical Separation of Identifiers

The foundational security principle of the IDIA Protocol is the physical and cryptographic separation of the user identity from the commercial data payload. Direct Identifiers (such as names, government identification, and exact biometric templates) never enter *The IDIA Hub* data lake. They remain cryptographically sealed within the hardware Secure Enclave or Keystore of the Sovereign Node at the edge. The Synapse Engine and Crazy Friend AI and the Crazy 8 security agents (while third-party enterprise datasets are sanitized via The Vulture pipeline) act as the ultimate fail-safe, programmatically scrubbing any rogue identifiers that attempt to cross the network boundary. The enterprise buyer receives only the pseudonymized operational telemetry bound to its respective ACA.

2. Strict Data Minimization

The IDIA Synapse Engine enforces strict data minimization protocols. The system ingests only the specific telemetry vectors required to fulfill the active, consented commercial purpose. If a Sovereign Node authorizes the sharing of point-of-sale volume data via *IDIA Pay*, the protocol does not covertly capture spatial location or unrelated biometrics. Ingestion is mathematically constrained to the exact parameters defined within the ACA.



3. Role-Based Access Controls (RBAC) and The Crazy 8 Suite

Access to the IDIA data infrastructure is governed by zero-trust architecture.

- **Internal Controls:** IDIA Data Inc. engineers operate under principle-of-least-privilege access, managed via AWS Identity and Access Management (IAM) and PostgreSQL Row-Level Security (RLS).
- **External Controls:** Enterprise buyers accessing *The IDIA Hub* are constrained by the *Crazy 8* security suite. Whether querying via standard SQL interfaces or the Model Context Protocol (MCP) bridge, autonomous agents and enterprise analysts are cryptographically locked into designated data vaults, preventing lateral movement or unauthorized dataset cross-referencing.

The "Crazy 8" functions as a decentralized suite of eight autonomous security agents within the IDIA Protocol, acting as the execution layer for the system's security posture. Governed by the Crazy Friend AI orchestrator and triggered directly by the Synapse Engine, the agents are divided into four distinct operational classes:

The Watchers (Class-S)

- **Sentinel:** Conducts continuous, real-time pattern monitoring across the ecosystem.
- **Gatekeeper:** Manages Identity and Access Management (IAM) triggers and enforces perimeter defense.

The Analysts (Class-A)

- **Oracle:** Handles predictive vulnerability forecasting to anticipate potential network exploits.
- **Insight:** Translates complex security telemetry into human-readable narrative explainability.

The Defenders (Class-D)

- **Shield:** Operates the Data Loss Prevention (DLP) protocols to ensure strict data boundary enforcement.
- **Mirror:** Provides adversarial detection, actively countering deepfakes, synthetic spoofing, and malicious injection attempts.



The Hunters (Class-H)

- **Hunter:** Conducts proactive threat hunting, continuously scanning the network for Indicators of Compromise (IoCs).
- **Guardian:** Executes automated Security Orchestration, Automation, and Response (SOAR) remediation to neutralize verified threats without requiring manual intervention.

Crazy Friend AI: Paranoid Autonomous Protection

To safeguard the Sovereign Node from malicious exploitation, bot-driven reconnaissance, and unauthorized data interception, the IDIA Protocol deploys *Crazy Friend AI*. Developed by leading minds in artificial intelligence, cryptography, and cyber operations, this decentralized security agent network acts as an unyielding sentinel across the user's data vault. Operating at the edge, Crazy Friend AI continuously monitors telemetry pipelines, neutralizes adversarial injection attacks, and enforces strict cryptographic isolation before any Zero-Knowledge Proofs or metadata are transmitted to The IDIA Hub. By embedding paranoid, hyper-vigilant autonomous defense directly into the user interface, the protocol ensures that Sovereign Nodes remain entirely insulated from corporate scraping, deepfake spoofing, and digital bad actors.

4. Retention Limits and Automated Purging

IDIA does not operate as a perpetual data hoard. All ingested telemetry is subject to strict Time-to-Live (TTL) retention policies dictated by the applicable ACA and regulatory requirements. Upon the expiration of a commercial license, or the moment a contributor revokes their consent, the IDIA Synapse Engine executes an automated cryptographic purge. The targeted dataset is systematically deleted from the active commercial lake, ensuring that stale or un-consented data is never exposed to the market or retained as an unfunded liability.

4.4 Egress Risk Assessment: The T-1-P Technical Vetting Protocol

The IDIA Protocol does not authorize the blind egress of raw data bundles to external enterprise environments. Before any quantitative fund, insurer, or federal agency is permitted to ingest raw, high-fidelity data from *The IDIA Hub*, the enterprise buyer must successfully pass the T-1-P Technical Vetting Protocol. This mandatory compliance and feasibility audit ensures the destination environment is technologically capable of maintaining IDIA's rigorous privacy and liability standards.

1. The Schema Audit and Liability Preservation

To ensure the enterprise liability shield survives the data transfer of a raw bundle, IDIA Sales Engineers execute a structured ingestion test. The client's Extract, Transform, and Load (ETL) pipeline must demonstrate the ability to process IDIA data payloads without stripping critical



metadata. The client must successfully ingest and persistently store both the Auditable Consent Artifact ID (`aca_record_id`) and the `X-IDIA-LIABILITY-TOKEN` header. If a client system strips this metadata during ingestion, it severs the chain of custody and fails the audit.

2. The Re-Identification Block

To neutralize the Mosaic Effect at the destination, the T-1-P audit mandates a strict review of the client's database architecture. The enterprise buyer must demonstrate a technical inability to join the IDIA `pseudonymized_user_id` against their internal Personally Identifiable Information (PII) tables (such as pre-existing customer emails or phone numbers).

3. Security Lineage and Retention Alignment

The vetting process verifies that the enterprise buyer enforces AES-256 encryption at rest across their storage volumes. Furthermore, the client must verify that their internal audit logs are retained for a minimum of one year, ensuring the technical infrastructure aligns precisely with the duration of the IDIA conditional indemnification terms.

4. Veto Authority and Contractual Hold (T-2-R)

The successful completion of the T-1-P protocol is the mandatory mechanism that unlocks the Conditional Indemnification Clause in the Master Service Agreement. If an enterprise buyer fails any critical metric of the audit, IDIA executes a Technical Remediation Request (Form T-2-R), placing the contract on a mandatory hold. The IDIA Protocol explicitly denies raw data egress and assumes zero liability for any external data processing until the client engineers remediate the blocking issues and successfully recertify their technical environment.

4.5 Data Fidelity, Hardware Variance, and Algorithmic Derivations

To establish clear operational boundaries and mitigate enterprise liability, the IDIA Protocol enforces strict legal definitions regarding the baseline accuracy of ingested telemetry and the predictive nature of its diagnostic indices. Enterprise buyers accessing *The IDIA Hub* must acknowledge and accept the following structural realities of decentralized edge data:

1. Hardware Variance and Sensor Limitations

The IDIA Protocol ingests telemetry from a vast array of independent Sovereign Nodes utilizing disparate Original Equipment Manufacturer (OEM) hardware (such as Apple Watch sensors, Zebra TC58 enterprise devices, or third-party POS terminals). Sensor calibration, native operating system background polling rates, and physical hardware degradation vary significantly across these devices. While the IDIA protocol normalizes the inbound schema, the foundational fidelity of the data remains strictly bound by the physical constraints and accuracy of the source hardware.



2. "As-Is" Data Presentation

All Licensed Data Assets and raw data bundles are provided to the enterprise buyer strictly on an "as-is" and "as-available" basis. The IDIA Synapse Engine executes rigorous cryptographic sanitization, schema normalization, and malicious payload rejection. However, the protocol cannot independently recalibrate external OEM sensors or definitively verify the physical reality of the ingested event (for example, differentiating between a physiological cardiac anomaly and a loose wearable strap). IDIA explicitly disclaims any warranty regarding the absolute scientific accuracy of the raw edge telemetry.

3. Subjective Nature of Derived Indices

The protocol generates advanced operational metrics, explicitly including the Human Reliability Index (HRI) and the Business Health Index (BHI). Enterprise buyers must legally recognize that these metrics are proprietary algorithmic derivations and predictive probabilities, not absolute objective facts.

- The **Human Reliability Index (HRI)** evaluates biological uptime and operational readiness based on telemetry inputs; it does not constitute a medical diagnosis, an absolute guarantee of future human performance, or a definitive physiological assessment.
- The **Business Health Index (BHI)** measures commercial velocity and margin stability; it does not constitute formal financial advice or a guarantee of corporate solvency.

The enterprise buyer assumes total legal and financial responsibility for how these predictive indices are weighted, interpreted, and deployed within their internal quantitative models, insurance underwriting frameworks, or risk assessment algorithms.

4.6 Biometric Data Storage and Ephemeral HRI Processing

To satisfy the compliance requirements of highly regulated enterprise environments and mitigate the risk of biological profiling, the IDIA Protocol enforces a strict architectural bifurcation between the persistent storage of foundational biometric telemetry and the temporary processing of derived operational indices.

1. Persistent Storage of Biometric Telemetry

Raw biometric telemetry (such as mobility cadence, gait asymmetry, and heart rate variability) is persistently stored within the IDIA infrastructure exactly like all other operational data. Upon generation by the Sovereign Node, the telemetry is cryptographically bound to its specific Auditable Consent Artifact (ACA). Direct Identifiers (PII) are permanently decoupled at the edge via local hardware enclave isolation prior to transmission. The resulting privacy-safe payload is



then securely warehoused within encrypted cloud environments (AWS GovCloud or commercial S3 data lakes). This persistent storage ensures data availability for enterprise licensing, but it remains strictly subject to the Time-to-Live (TTL) retention limits and commercial restrictions dictated by the contributor active consent parameters.

2. Ephemeral Processing of the Human Reliability Index (HRI)

In direct contrast to persistent telemetry storage, the Human Reliability Index (HRI) does not function as a long-term historical ledger. The HRI is engineered exclusively as a real-time diagnostic metric evaluating immediate biological uptime and operational readiness.

Consequently, HRI scores are calculated dynamically and processed temporarily in memory by our AI. Once the real-time operational state is verified or the immediate enterprise query is satisfied, the specific HRI diagnostic score is not persistently warehoused as a permanent historical record. This ephemeral processing architecture protects the Sovereign Node; it ensures that contributors are evaluated solely on their current operational capacity and cannot be algorithmically penalized by stale, historical fatigue metrics during future licensing events.

4.7 Security Architecture, Incident Response, and Independent Auditing

To protect the integrity of the Verified Truth Economy, the IDIA Protocol deploys a comprehensive security architecture governing data access, encryption, and operational incident response.

1. Encryption, Audit Trails, and Access Permissions

All data at rest within the IDIA infrastructure is secured utilizing AES-256 encryption, while data in transit is protected via TLS 1.3 cryptographic protocols. Internal access to the IDIA Synapse Engine and cloud infrastructure operates strictly under principle-of-least-privilege Role-Based Access Controls (RBAC), enforced through AWS Identity and Access Management (IAM) and PostgreSQL Row-Level Security (RLS). Furthermore, the *Crazy 8* security suite—driven by *Crazy Friend AI* at the edge—continuously monitors the network perimeter for anomalous query behavior and unauthorized access attempts. The protocol maintains an immutable internal audit trail of all administrative actions, data sanitization events, and enterprise data transfers.

2. Incident Response and Breach Notification Responsibilities

Should the security network detect a potential intrusion or unauthorized exposure of pseudonymized data, Crazy Friend AI executes a formalized incident response protocol, notifying IDIA staff in real-time. IDIA is committed to fulfilling all statutory breach notification responsibilities subject to applicable law. In the event of a verified breach, affected Sovereign Nodes, enterprise buyers, and relevant regulatory authorities will be notified without undue delay



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

—and strictly within the timeframes mandated by applicable legal frameworks—detailing the scope of the exposure and the exact technical remediation actions deployed.

3. Status of Independent Security Assessments

While IDIA maintains rigorous internal security validation and edge-level cryptographic isolation, the company adheres to strict transparency standards regarding external certifications. As of the current pilot development phase, formal, independent third-party security certifications (such as SOC 2 Type II compliance or external smart-contract penetration test reports) are pending. Comprehensive external security audits and formal regulatory compliance reviews are scheduled as a primary use of proceeds from the Seed capital deployment. IDIA will obtain these independent certifications prior to initiating national commercial scaling or concluding Federal enterprise procurement.

Section 5

COMMERCIAL MODEL & ENTERPRISE LICENSING**5.1 Target Enterprise Verticals and Initial Commercial Use Cases**

The IDIA Protocol bypasses commoditized advertising networks to directly target high-consequence enterprise sectors. These initial verticals suffer from severe liability exposure and require cryptographically verified, Zero-PII ground truth to maintain operational solvency.

1. Commercial Logistics and Fleet Operations (Trucking)

- **The Problem:** Fleet operators face compounding insurance premiums and catastrophic liability resulting from driver fatigue and operational negligence.
- **The IDIA Use Case:** Utilizing the Cognitive Performance Module (CPM) and the Human Reliability Index (HRI) via *Life by IDIA*, logistics companies can monitor the real-time biological uptime and cognitive readiness of their fleet operators. By proving drivers are biologically fit before dispatch, operators can negotiate reduced insurance premiums, while drivers receive direct performance royalties for maintaining their operational readiness.

2. Intellectual Property and Digital Rights Administration

- **The Problem:** The proliferation of synthetic media and unauthorized artificial intelligence training has destroyed traditional copyright enforcement, leaving creators uncompensated for the ingestion of their digital assets.
- **The IDIA Use Case:** Operating on the music publishing administration blueprint, the protocol manages complex provenance, auditable consent, and programmatic performance royalties for intellectual property. IDIA acts as the administrative clearinghouse, ensuring that every time an enterprise consumes a registered digital asset or audio fingerprint, the usage is verified and a royalty is automatically routed to the sovereign creator.

3. Frontier Artificial Intelligence and Machine Learning

- **The Problem:** Foundation models are experiencing "Model Collapse" due to the ingestion of unverified synthetic data (AI Slop) and unauthorized web scraping, which introduces massive copyright liability.
- **The IDIA Use Case:** Enterprise artificial intelligence developers purchase cryptographically authenticated human telemetry from *The IDIA Hub* to inoculate their

training pipelines. The protocol provides the legally indemnified, human-anchored ground truth necessary to train models safely without violating global privacy mandates.

4. Algorithmic Trading and Quantitative Finance

- **The Problem:** Alpha generation requires alternative data, but utilizing scraped consumer data exposes hedge funds to severe regulatory action from the Securities and Exchange Commission (SEC).
- **The IDIA Use Case:** Quantitative desks utilize the protocol to access high-velocity, pseudonymized commercial data (such as point-of-sale volume from *IDIA Pay* merchants) to inform algorithmic trading strategies, fully protected by the IDIA conditional liability shield.

5.2 The Enterprise Deliverable: Licensed Data Assets

To execute commercial transactions across these verticals, IDIA Data Inc. does not sell access to a monolithic, unstructured database. Enterprise buyers execute Master Service Agreements to procure strictly defined, technically formatted deliverables known as Licensed Data Assets.

The enterprise buyer procures data through *The IDIA Hub* in the following specific formats:

- 1. Continuous Feature Feeds (API and WebSocket)** Low-latency data streams delivering real-time, pseudonymized operational metrics and derived indices (such as the Business Health Index). These feeds integrate directly into enterprise risk models and quantitative trading algorithms requiring microsecond execution.
- 2. Model Context Protocol (MCP) Ingestion** Standardized context feeds engineered specifically for autonomous artificial intelligence agents. The MCP bridge allows authorized enterprise agents to query the protocol for verified human context, providing the agent with the "Ground Truth" necessary to execute high-liability decisions safely.
- 3. Aggregated Statistical Bundles** Macro-level, parameterized SQL extracts compiling pseudonymized records into geographic, temporal, or behavioral cohorts. These bundles provide macro-intelligence for urban planners, real estate developers, and insurers without exposing individual node telemetry.
- 4. Raw Telemetry Bundles (T-1-P Gated)** In scenarios requiring deep analytical modeling, enterprise buyers may procure bundles of raw, pseudonymized telemetry. However, as previously established, the egress of these high-fidelity bundles is strictly gated behind the successful execution of the T-1-P Technical Vetting Protocol, ensuring the buyer possesses the database architecture required to prevent the Mosaic Effect and maintain the enterprise liability shield.

5.3 Revenue Architecture: Subscriptions, Licensing, and Metered Usage

The IDIA Protocol generates revenue through a "Double-Helix" architecture, separating high-margin recurring SaaS revenue from scalable, consumption-based data clearing fees. This structure ensures platform sustainability while aligning incentives between the network and its contributors.

1. Sovereign Node Subscriptions (SaaS)

- **Mechanism:** Recurring monthly subscription fees paid by individuals and merchants to access advanced operational tooling and local analytics.
- **Deliverable:** Premium access to *Life Pro* (\$9.99/mo), *Life Pro+* (\$49.99/mo), *Pure Alpha* (\$99.99/mo), and *IDIA Pay Pro* (\$49.99/mo). These tiers provide local access to continuous HRI diagnostics, Business Health Index scoring, and embedded operational software.
- **Economic Treatment:** Subscription revenue is recognized entirely as corporate operating revenue for IDIA Data Inc. and is not subject to the data royalty split.

2. Enterprise Platform Subscriptions (Access Licensing)

- **Mechanism:** Annual licensing fees paid by institutional buyers for authenticated access to *The IDIA Hub*.
- **Deliverable:** Platform access tiers ranging from Analyst (\$9,995/year) to Enterprise (\$49,995+/year), providing the buyer with the legal Master Service Agreement (S-3-C), integration support, and access to the enterprise liability shield.
- **Economic Treatment:** Platform access fees are recognized as corporate operating revenue for IDIA Data Inc.

3. Metered Data Consumption (Synapse Credits)

- **Mechanism:** The variable, consumption-based engine that monetizes the actual extraction of data. Enterprise buyers must expend Synapse Credits (\$0.75 per credit) to execute queries or maintain continuous feature feeds.
- **Deliverable:** The real-time delivery of the Licensed Data Assets (API payloads, MCP agent context injections, or SQL bundle extracts).
- **Economic Treatment:** This metered consumption constitutes the "Licensing Pool." This is the exclusive revenue stream subject to the programmatic royalty split (60% to Platform Operations, 30% to Contributors, 10% to the Decentralized War Chest).

5.4 The Billable Event: Defining "Qualifying Commercial Use"

To ensure absolute transparency in royalty accounting, the IDIA Protocol abandons opaque data-broker revenue sharing models. A royalty is generated exclusively by a mathematically verifiable, on-chain event, ensuring compensation relies on strict deterministic execution rather than ambiguous definitions of "data value" or fractional ownership of massive databases.

The Synapse Credit Consumption Event

A royalty is triggered exclusively when an enterprise buyer executes a "Qualifying Commercial Use." Within the protocol, this is defined as the exact millisecond the IDIA Synapse Engine successfully deducts a Synapse Credit from an enterprise buyer's funded treasury vault to fulfill a data request.

- **API / SQL Execution:** When an enterprise algorithm queries a specific point-of-sale aggregate or biometric cohort, the Synapse Engine identifies the individual Sovereign Nodes whose Auditable Consent Artifacts (ACAs) comprise that specific payload. As the Synapse Credit is consumed to deliver the payload, the protocol automatically logs a micro-transaction, attributing a fractional share of that consumed credit to the originating nodes.
- **MCP Agent Ingestion:** Similarly, when an autonomous artificial intelligence agent queries the protocol for "Ground Truth" context via the Model Context Protocol bridge, the successful delivery of that context payload triggers the credit consumption event, instantly crediting the Sovereign Nodes that provided the operational telemetry.

If data sits idle in the encrypted data lake, it generates zero yield. The protocol compensates active commercial utility, ensuring that royalty distributions are always fully funded by verified, real-time enterprise consumption.

5.5 Contribution Attribution and Dynamic Valuation Weighting

When a Synapse Credit consumption event occurs, the protocol must execute a precise, mathematically auditable distribution of the resulting revenue. Because data possesses varying levels of fidelity and commercial value, the IDIA Protocol utilizes the IDIA Synapse Engine to dynamically weight and calculate contributor allocations.

1. The Standard Allocation Split

Every consumed Synapse Credit (\$0.75) initiates a programmatic split hardcoded into the Synapse Engine routing: 60% (\$0.45) is allocated to Platform Infrastructure (IDIA Data Inc.), 30% (\$0.225) is directed to the Contributor Royalty Split, and the remaining 10% (\$0.075) funds the Decentralized Community Grant Pool (the localized "War Chest").



2. The Synapse Weighting Algorithm (0.1 to 1.0)

The 30% Contributor Royalty Split is not distributed as a flat, egalitarian dividend. The Synapse Engine acts as the valuation layer, assigning a dynamic coefficient (ranging from 0.1 to 1.0) to every specific data payload involved in the enterprise query. This coefficient is calculated based on three core vectors:

- **Fidelity and Granularity:** Raw, high-frequency telemetry (Tier-0 mapped to an ACA) receives a higher coefficient than diluted, macro-aggregated statistics.
- **Operational Readiness:** Telemetry originating from a Sovereign Node maintaining high Biological Uptime (HRI) or a high Trust Score commands a premium valuation, as the data represents a more reliable "Ground Truth."
- **Temporal Relevance:** Live, real-time data streaming to a quantitative desk receives a higher weight than archived, historical telemetry.

3. Pro-Rata Distribution

The Synapse Engine calculates the total cumulative weight of all ACAs utilized in the specific enterprise query, and distributes the \$0.225 fractional royalty pro-rata based on each node's exact algorithmic contribution. This ensures that contributors maintaining high-quality, continuous, and verified operational telemetry receive the highest commercial yield.

5.6 Fractional Distributions, Deduplication, and Settlement Thresholds

Processing commercial licenses for aggregated datasets requires managing millions of micro-transactions across overlapping contributor cohorts. The IDIA Protocol enforces strict operational rules to manage scale, prevent fraud, and handle attribution disputes.

1. Multiple Contributors and Overlapping Datasets

When an enterprise buyer procures a macro-aggregated bundle, the query may access data from thousands of individual Sovereign Nodes simultaneously. The Synapse Engine fractionalizes the Contributor Royalty Split across all verified ACAs mathematically bound to that payload. To prevent artificial yield inflation, the *Crazy 8* security suite enforces strict deduplication protocols; if a Sovereign Node qualifies under multiple parameters of a single query, their data is consolidated and compensated as a single authorized contribution for that specific extraction event.

2. Disputed Attribution and Cryptographic Finality

In the event of an attribution anomaly or a dispute regarding royalty allocations, the protocol relies exclusively on cryptographic finality rather than subjective arbitration. The settlement of a



data purchase mints a soulbound IDIALiabilityReceipt on the Base Layer-2 network. This receipt immutably records the exact ACA hashes of the contributing users. If a royalty is disputed, the ledger serves as the absolute, mathematically verifiable arbiter of which node provided the data at the exact millisecond of consumption.

3. Minimum Payout Thresholds and Batch Settlement

Gas-Sponsored Instantaneous L2 Settlement: Utilizing the low-cost execution environment of the Base Layer-2 network alongside platform-sponsored gas relayers, the IDIA Protocol eliminates network fee attrition on micro-transactions. Rather than subjecting contributors to delayed batch thresholds, fractional royalties are settled instantaneously: the moment a Synapse Credit is consumed, the exact pro-rata USDC royalty is transferred directly to the contributor's non-custodial Base Layer-2 wallet."

5.7 Enterprise Buyer Restrictions and Data Lifecycle Obligations

The acquisition of a Licensed Data Asset through *The IDIA Hub* does not grant the enterprise buyer perpetual ownership or unrestricted commercial liberty over the dataset. All transactions are governed by the Master Service Agreement (S-3-C), which imposes rigorous restrictions, downstream limitations, and mandated deletion obligations.

1. Sub-Licensing and Downstream Prohibition

Enterprise buyers are strictly prohibited from reselling, sub-licensing, or commercially redistributing raw or pseudonymized IDIA datasets to unauthorized third parties. The license granted is expressly restricted to internal enterprise utilization, quantitative modeling, and proprietary artificial intelligence training.

2. Retention Limits and Mandated Deletion

Every Licensed Data Asset is bound by a Time-to-Live (TTL) parameter dictated by the originating Auditable Consent Artifact (ACA). Upon the expiration of the licensed term, or upon the formal revocation of a user's consent, the enterprise buyer is legally obligated to execute a systemic purge of the specific data records from their internal servers. IDIA Data Inc. reserves the right to audit the buyer's compliance and demand a formalized Certificate of Destruction.

5.8 Revenue Recognition: Contracted vs. Prospective Pipeline

To maintain absolute financial transparency for institutional investors and regulatory auditors, IDIA Data Inc. strictly demarcates recognized commercial revenue from projected, uncontracted pipeline opportunities.



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

1. Recognized Contracted Revenue

Revenue is formally recognized only when an enterprise buyer executes a Master Service Agreement and physically funds their treasury vault with fiat or digital assets to mint Synapse Credits. Furthermore, the 30% Contributor Royalty Split is classified strictly as a pass-through liability; IDIA Data Inc. recognizes only the 60% Platform Infrastructure fee and the direct SaaS subscription revenues as corporate operating income.

2. Prospective and Uncontracted Pipeline

Memorandums of Understanding (MOUs), Letters of Intent (LOIs), and active pilot discussions (such as regional logistics partnerships or municipal integration talks) are classified strictly as prospective pipeline. These figures are explicitly excluded from booked Annual Recurring Revenue (ARR) calculations until the technical integration is completed and the enterprise buyer initiates live Synapse Credit consumption.

5.9 Zero-Trust Query Resolution and Permission Boundaries

Enterprise demand frequently intersects with the boundaries of contributor privacy. When an institutional buyer or an autonomous AI agent submits a query to *The IDIA Hub* that exceeds the explicitly granted permissions of the underlying Sovereign Nodes, the protocol employs a Zero-Trust Query Resolution process.

Dynamic Truncation and Rejection

The IDIA Synapse Engine programmatically cross-references every inbound enterprise query against the active ACA ledger. To enforce user preferences regarding restricted data vectors (such as precise location), the protocol dynamically truncates the payload and returns exclusively the specific data fields that possess cryptographic authorization. If the entirety of the query violates the consent parameters, the payload is rejected outright, the Synapse Credit is not consumed, and the enterprise buyer is notified of the permission boundary restriction.



Section 6

ROYALTY ECONOMICS & FINANCIAL SETTLEMENT

6.1 Asset Taxonomy: Synapse Credits, USDC, and Governance Tokens

To ensure regulatory compliance and operational clarity, the IDIA Protocol utilizes a tri-asset architecture. Each asset performs a strictly segregated function within the economic lifecycle, separating API metering from financial settlement and network governance.

1. Synapse Credits (The Metering Unit) Synapse Credits are strictly internal, consumable access units utilized exclusively by enterprise buyers to meter data extraction. They are fiat-pegged at a fixed rate of \$0.75 per credit. Synapse Credits are not cryptocurrencies, they are not redeemable for cash by the purchaser, and they are strictly non-transferable between enterprise accounts. They function solely as a secure accounting mechanism to track Best Friend AI and API utilization and Model Context Protocol (MCP) data consumption within *The IDIA Hub*.

2. USDC Stablecoin (The Settlement Layer) While enterprise consumption is metered in Synapse Credits, the financial settlement to the Sovereign Node is executed in USDC (USD Coin). Operating on the Base Layer-2 network, USDC provides a liquid, regulated, fiat-backed medium of exchange. When a Synapse Credit is consumed, the resulting fractional royalty is aggregated and ultimately distributed as USDC directly to the contributor's non-custodial wallet. This mechanism ensures that data yields hold immediate, real-world purchasing power without exposing the contributor to the volatility of speculative crypto-assets.

3. IDIA Governance Token (The Ownership Layer) The IDIA Governance Token (an ERC-20 token deployed on the Base network) represents the decentralized voting and administrative layer of the IDIA Protocol. It is mathematically decoupled from the financial clearing price of the data. However, to ensure that the network is governed by its active participants, IDIA Governance Tokens are programmatically distributed to data contributors commensurate with their verified data yield. This dual-distribution architecture effectively grants active data producers a direct, voting voice within the protocol's Decentralized Unincorporated Nonprofit Association (DUNA).

6.2 Hypothetical Revenue Allocation Model

To demonstrate the accounting logic of the IDIA Synapse Engine, the following table provides a theoretical transaction model. *Note: The following figures are strictly hypothetical and are intended solely for illustrative purposes to demonstrate the programmatic execution of the 60/30/10 split. They do not constitute financial projections or guarantees of actual corporate revenue.*

Illustrative Enterprise Transaction: An enterprise artificial intelligence developer deposits fiat into their treasury vault to procure 1,000 Synapse Credits (\$750.00). The developer's



autonomous agent executes a series of queries that successfully consume all 1,000 credits, extracting context parameters originating from a cohort of verified Sovereign Nodes.

Gross Transaction Volume: \$750.00 (1,000 Synapse Credits Consumed)

Programmatic Settlement:

- **Platform Infrastructure (60% Allocation): \$450.00**
 - *Function:* Routed to IDIA Data Inc. corporate accounts to fund cloud infrastructure, edge-node maintenance, API execution, and corporate operations.
- **Contributor Royalty Split (30% Allocation): \$225.00**
 - *Function:* Routed to the settlement ledger to be distributed in USDC among the specific Sovereign Nodes that provided the data. The exact distribution of this \$225.00 is fractionalized pro-rata across the cohort based on the Synapse Engine weighting algorithm (0.1 to 1.0) applied to each underlying Auditable Consent Artifact (ACA).
- **Decentralized Community Grant Pool / War Chest (10% Allocation): \$75.00**
 - *Function:* Routed to the appropriate `IDIA_LocalizedPool.sol` regional treasury vault on the Base network. This localized capital is governed by the regional DAO to fund community initiatives and localized infrastructure within the jurisdiction where the data was generated.

6.3 Custody Architecture: Reception, Transmission, and Settlement of Funds

The administration of enterprise licensing revenue requires clear delineation of institutional custody and transmission authority across both fiat and decentralized rails. The IDIA Protocol enforces structural segregation among the entities responsible for receiving, holding, and distributing capital:

1. Capital Ingestion and Holding

Enterprise capital enters the ecosystem through two primary conduits:

- **Fiat Procurement:** Enterprise buyers procuring annual platform subscriptions or purchasing Synapse Credits via traditional currency transfer funds directly to commercial operating accounts maintained by IDIA Data Inc. with insured domestic banking partners. IDIA Data Inc. serves as the central billing counterparty and Authority of Record under the Master Service Agreement.



- **Digital Asset Procurement:** Enterprise buyers settling directly in digital currency deposit USDC on the Base Layer-2 network into authenticated smart contract vaults. These digital assets are safeguarded within enterprise multi-signature architecture (managed via Gnosis Safe) requiring multi-party authorization across executive keyholders.

2. Transmission Authority and Administrative Agency

IDIA Data Inc. does not function as a custodial bank or a deposit broker. The transmission of data royalties to Sovereign Nodes operates strictly under the Limited Power of Attorney (LPOA) and administrative agency granted during device registration. IDIA Data Inc. acts solely as an administrative clearing agent: calculating the programmatic 60/30/10 split, withholding the corporate platform fee, and routing the net licensing proceeds to the entitled contributors and regional treasuries.

3. Contributor Settlement

Sovereign Nodes maintain absolute custody of their distributed yields. The protocol transmits contributor royalties directly to the non-custodial Base Layer-2 wallet initialized within the *Life by IDIA* mobile client. Data contributors retain sole cryptographic control over their private keys and are alone authorized to hold, transfer, or off-ramp their accumulated USDC.

6.4 Banking Partners, Payment Processors, and Smart Contract Architecture

The execution of continuous, micro-fractional settlements requires synchronized interoperability between traditional banking rails and autonomous on-chain smart contracts.

Settlement Phase	Ingress / Routing Mechanism	Designated Destination & Function
1. Treasury Funding	Fiat Ingress (Cards / ACH / Wire)	Acquiring Processors & Partner Banks: Handles KYC/AML and corporate payment acceptance.
	Digital Ingress(USDC on Base L2)	Gnosis Safe Multisig Treasury: Secures enterprise digital asset deposits via multi-signature architecture.
2. Event Trigger	Synapse Engine Settlement	Automated Pipeline: Verifies credit consumption and executes programmatic distribution arrays.
3. The 60/30/10 Split	60% (Platform Infrastructure)	IDIA Data Inc. Accounts: Funds cloud infrastructure, API execution, and operations.
	30% (Contributor Split)	Life by IDIA Wallets: Direct Base L2 USDC transfer to the specific Sovereign Nodes that provided the data.
	10% (Community War Chest)	IDIARegistry.sol → IDIA_LocalizedPool.sol: Routes capital to the specific regional DAO treasury where the data was generated.



1. Commercial Acquiring and Fiat Gateways

Commercial payment processing partners and licensed acquiring institutions facilitate enterprise credit card and Automated Clearing House (ACH) billing. These partner institutions handle the compliance, Know Your Customer (KYC), and Anti-Money Laundering (AML) checks required for corporate payment acceptance, shielding the protocol from fraudulent payment vectors.

2. The Synapse Engine Settlement Pipeline

As queries execute against *The IDIA Hub*, backend functions verify credit availability, calculate record weighting coefficients, and orchestrate the tripartite revenue distribution. These functions trigger simultaneous fiat ledger updates and on-chain contract executions.

3. Smart Contract Execution Rails (Base Layer-2)

- **IDIALiabilityReceipt.sol**: Upon successful settlement, the controller mints a soulbound, non-transferable ERC-721 token to the enterprise buyer's designated address. This token immutably anchors the transaction reference, the purchased data bundle identifier, and the exact Auditable Consent Artifact (ACA) cryptographic hashes of the contributing nodes.
- **IDIAEscrow.sol**: Multi-signature escrow vaults govern the scheduled release and distribution of IDIA Governance Tokens, ensuring network ownership distributions align strictly with validated data contributions.
- **IDIARegistry.sol** and **IDIA_LocalizedPool.sol**: The settlement pipeline queries the **IDIARegistry** contract to match the contributor location metadata against deployed regional pools. The 10% decentralized community allocation is automatically routed to the corresponding **IDIA_LocalizedPool** contract, preserving capital for local infrastructure within the jurisdiction that produced the data.

6.5 Transaction Fees, Reversals, Fraud Adjustments, and Settlement Timing

To safeguard ecosystem liquidity and prevent financial exploitation, the IDIA Protocol enforces rigorous settlement parameters governing processing friction, transaction disputes, and distribution schedules.

1. Transaction Fees and Network Gas

- **Blockchain Network Gas**: Base Layer-2 transaction fees incurred during internal processing and instantaneous royalty disbursements are absorbed directly by IDIA Data Inc. through platform infrastructure reserves or sponsored transaction relayers. Contributors do not pay gas fees to receive their earned USDC royalties.



- **Off-Ramp Conversion Fees:** When an individual or merchant contributor chooses to off-ramp USDC into external fiat banking rails, standard third-party network processing fees (approximately 1.5%) apply at the gateway level.

2. Enterprise Purchase Finality, Reversals, and Chargebacks

The consumption of Licensed Data Assets constitutes the delivery of an immediate, non-recoverable digital performance.

- Once a Synapse Credit is consumed to execute an API call, deliver an MCP agent context payload, or export a query dataset, the transaction is irreversible and final.
- In the event an enterprise buyer initiates an unauthorized payment reversal or card chargeback through an external bank, the IDIA Synapse Engine instantly suspends the buyer's API credentials, voids the active Master Service Agreement, and invalidates the associated IDIALiabilityReceipt.
- Because enterprise accounts require verified onboarding and treasury pre-funding, chargeback exposure is isolated to corporate reserves; contributor balances are insulated from retroactive clawbacks resulting from buyer default.

3. Telemetry Fraud Adjustments and Sanitization

Telemetry streams are continuously evaluated by the *Crazy 8* security suite prior to credit allocation.

- If the system detects synthetic spoofing, simulated mobility patterns, bot-driven POS manipulation, or replay attacks, the anomalous data is rejected at the perimeter.
- Sovereign Nodes flagged for malicious or fraudulent telemetry generation forfeit any pending or accrued Synapse Yield tied to the fraudulent records. The forfeited proceeds are routed to the platform reserve to offset audit and remediation overhead.

4. Instantaneous Settlement Latency and Payout Timing

The IDIA Protocol explicitly rejects the legacy data-broker model of delayed net-30 payouts.

- **Real-Time On-Chain Execution:** The distribution of the Contributor Royalty Split is instantaneous. The moment a Synapse Credit is consumed by an enterprise buyer the Synapse Engine executes the transaction on the Base Layer-2 network.
- **Immediate Custody:** The liquid USDC distribution is transferred instantaneously to the verified Sovereign Node's non-custodial wallet, ensuring that the contributor has

immediate cryptographic ownership and operational liquidity the exact millisecond their data performance is rendered.

6.6 Treasury Governance, Reserves, and Automated Reconciliation

To maintain the integrity of the Verified Truth Economy, IDIA Data Inc. enforces rigorous treasury management protocols, ensuring absolute separation between corporate operating funds, enterprise digital asset deposits, and decentralized community capital.

1. Treasury Custody and Governance Controls

- **Enterprise Digital Deposits:** Enterprise buyers funding their vaults with USDC are routed into secure multi-signature treasury contracts managed via the Gnosis Safe architecture. The movement of bulk enterprise capital requires multi-party cryptographic authorization from designated IDIA Data Inc. executive keyholders, preventing unilateral access or localized credential compromise.
- **Decentralized War Chests:** The 10% localized community grant allocations are routed directly to non-custodial `IDIA_LocalizedPool.sol` contracts. IDIA Data Inc. explicitly surrenders unilateral withdrawal authority over these regional vaults; capital deployment requires formal governance proposals and on-chain execution by the respective regional Decentralized Unincorporated Nonprofit Association (DUNA).

2. Automated Ledger Reconciliation and Reporting

The IDIA Protocol eliminates the need for manual end-of-month royalty reconciliation. Every instantaneous settlement executed by the Synapse Engine is simultaneously recorded across a dual-ledger architecture:

- **Off-Chain Ledger:** The internal PostgreSQL database updates the `ActivityLedger` and `ProvenanceAuditLog`, mapping the exact Synapse Credit consumption event (e.g., `SYN-371E8458`) to the specific `aca_hash_key`.
- **On-Chain Ledger:** The Base Layer-2 network records the immutable USDC transfer to the Sovereign Node.

This dual-entry system allows IDIA Data Inc. to programmatically generate real-time, mathematically verifiable transparency reports for enterprise buyers and regulatory auditors, proving exact chain-of-custody for every fraction of a cent distributed.



6.7 Regulatory Boundaries: Money Transmission, Securities, and Taxation

The IDIA Protocol operates within a highly regulated global financial ecosystem. To mitigate enterprise and corporate liability, IDIA Data Inc. enforces the following strict legal and regulatory boundaries, subject to ongoing review by external compliance counsel:

1. Money Transmission and Financial Services

IDIA Data Inc. operates fundamentally as an administrative software agent and data licensing clearinghouse, not as a chartered bank or a depository institution.

- **Fiat Operations:** All fiat payment processing, credit card acquiring, and external bank transfers are executed exclusively through licensed third-party Banking-as-a-Service (BaaS) partners and Payment Facilitators. IDIA relies on these partners to execute requisite Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance for fiat gateways.
- **Money Transmitter Licenses (MTL):** Where state statutes dictate that the specific routing of data licensing proceeds constitutes regulated money transmission, IDIA Data Inc. restricts direct operational authority pending the successful acquisition of the required Phase 1 State Money Transmitter Licenses (MTLs) and requisite surety bonds.

2. Digital Assets and Securities Compliance

The economic assets within the IDIA ecosystem are structurally decoupled to comply with global securities regulations (e.g., the Howey Test):

- **Synapse Credits** are non-transferable internal utility meters with zero speculative secondary market.
- **USDC** is a regulated, fiat-backed stablecoin utilized strictly as a medium of exchange.
- **The IDIA Governance Token** confers decentralized administrative voting rights within the DUNA; it explicitly does not represent corporate equity, shareholding rights, or an expectation of corporate profit in IDIA Data Inc.
- **Series I Telemetry Units (\$SITs) and Perpetual Preferred Units**, utilized to capitalize the IDIA Indemnity Reserve, LLC, are formal securities offered strictly to accredited institutional investors under authorized exemptions (e.g., SEC Regulation D, Rule 506(c)).



3. Contributor Tax Implications and Substantiation

As established in the Sovereign Proprietorship model, data contributors act as independent commercial entities licensing their data through the platform.

- Contributors are solely responsible for calculating and remitting their applicable jurisdictional taxes on accrued Synapse Yields.
- To assist with Internal Revenue Service (IRS) compliance (specifically IRC §162 Deductions and §6001 Recordkeeping), *Life by IDIA* provides the "Pattern of Life (PoL) Ledger," acting as an automated substantiation log.
- IDIA Data Inc. complies with all federal reporting mandates, programmatically issuing 1099-K or 1099-MISC tax documents to contributors who exceed statutory gross revenue thresholds during the fiscal year.

6.8 Risk Mitigation: The Indemnity Treasury (IDIA Indemnity Reserve, LLC)

To address the structural fragility of legacy counterparty insurance and backstop the enterprise Liability Shield, the IDIA Protocol establishes a dedicated institutional risk vehicle: **IDIA Indemnity Reserve, LLC**.

1. Corporate Structure and Bankruptcy-Remote Purpose

IDIA Indemnity Reserve, LLC is a bankruptcy-remote Delaware Series Limited Liability Company managed by IDIA Data Inc. Its sole corporate mandate is to hold, custody, and manage the **Indemnity Reserve Assets**. These assets serve as the financial backstop for the Conditional Indemnification obligations granted to enterprise buyers under the IDIA Liability Shield (`IDIALiabilityReceipt.sol`). This legal segregation ensures that institutional "Risk Capital" is completely ring-fenced from the operating capital of IDIA Data Inc., insulating the reserve from corporate operational contagion.

2. Series I Telemetry Units (\$SITs) — Variable Usage-Backed Index

The **Series I Telemetry Units (\$SITs)** are uncertificated, book-entry security derivatives—offered exclusively to accredited investors under SEC Regulation D, Rule 506(c) and internationally via CIMA-regulated structures—that function as a usage-backed cash-flow index. Expressly decoupled from retail web3 or speculative token mechanics, \$SITs align institutional risk capital directly with the continuous velocity of verified human telemetry licensed through *The IDIA Hub*.

- **The \$0.25 Programmatic Sweep:** Unlike speculative digital assets, the valuation and variable yield of \$SITs are mathematically tethered to real-world platform throughput.

Specifically, \$SIT performance is driven by an automated **\$0.25 fiat reserve allocation sweep** triggered every time an enterprise buyer consumes a Synapse Credit on *The IDIA Hub*. This consumption telemetry feeds directly into the variable yield calculations of the \$SIT book-entry register, dynamically scaling distributions alongside verifiable enterprise licensing volume.

3. Series I Perpetual Preferred Units — Institutional Capital Bedrock

While \$SITs act as a variable-yield instrument tethered to Synapse Credit velocity, the **Series I Perpetual Preferred Units** serve as the foundational, fixed-yield capital anchor of IDIA Indemnity Reserve, LLC:

- **Institutional Capital Backing:** Designed to absorb heavy institutional allocations (Family Offices, Sovereign Wealth, and Institutional Endowments), seeding the baseline liquidity required to capitalize the indemnity reserve vaults.
- **10.00% Cumulative Preferred Return:** Carries a fixed **10.00% cumulative preferred return**, ensuring institutional backers hold a prioritized, predictable, and legally enforceable senior claim on reserve distributions before any junior ecosystem payouts occur.
- **Perpetual Duration:** Carries no fixed maturity date, remaining active perpetually within the capitalization table to provide permanent baseline liquidity backstopping marketplace transactions.
- **Regulatory Structure:** Issued under a dedicated Statement of Designation within the Delaware Series LLC framework pursuant to SEC Regulation D, Rule 506(c).

4. Reserve Capitalization, Seniority, and the "Shield" Covenant

The Statements of Designation governing both \$SITs and Series I Perpetual Preferred Units enforce strict fiduciary covenants:

- **Senior Ranking:** Both instruments rank senior to Common Units and any junior corporate equity.
- **The "Shield" Covenant:** Proceeds from the issuance of \$SITs and Series I Units must be held in a legally segregated **Reserve Vault** and are strictly prohibited from being commingled with IDIA Data Inc. corporate operating funds.
- **Permitted Uses & HQLA Mandate:** Reserve Vault capital may be deployed strictly for three authorized purposes:



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

1. Settlement of verified enterprise liability claims triggered by a valid IDIALiabilityReceipt event.
2. Payment of accrued 10.00% cumulative preferred returns and variable yields to Series I and \$SIT holders.
3. Deployment into **High-Quality Liquid Assets (HQLA)**, defined strictly as short-duration U.S. Treasury Bills or Investment-Grade Sovereign Debt.



Section 7

TOKENOMICS & TREASURY DESIGN

7.1 Asset Specification and Verifiable Supply

To provide absolute transparency to institutional buyers, regulatory bodies, and ecosystem participants, IDIA Data Inc. publishes the exact cryptographic specifications and allocation parameters of the network's administrative asset.

- **Official Token Name:** IDIA Governance Token
- **Network Deployment:** Base Mainnet (Layer-2)
- **Smart Contract Address:**
0x6526F939D257E67896821c25B6C24Daa404a01FB
- **Token Standard:** ERC-20 (extending OpenZeppelin ERC20Votes, ERC20Permit, and ERC20Burnable)
- **Maximum Supply:** 10,000,000,000 IDIA (Fixed supply, minted entirely at deployment)

Programmatic Supply Allocation The total fixed supply is distributed across five immutable IDIAEscrow.sol multi-signature vaults, programmed strictly according to the following capitalization table:

- **Liquidity & Staking (35%):** 3,500,000,000 IDIA
- **Ecosystem / Treasury (30%):** 3,000,000,000 IDIA (Utilized for programmatic contributor matching and network rewards)
- **Team & Advisors (15%):** 1,500,000,000 IDIA
- **Early Investors (10%):** 1,000,000,000 IDIA
- **Public Sale / Airdrop (10%):** 1,000,000,000 IDIA

7.2 Token Utility and On-Chain Governance Rights

The IDIA Governance Token functions exclusively as the decentralized administrative layer of the IDIA Protocol. It allows data contributors to actively manage the public-good infrastructure they power.



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

The Decentralized Unincorporated Nonprofit Association (DUNA)

Governance rights are administered through IDIA DAO LLC, which operates under Wyoming statutes as a Decentralized Unincorporated Nonprofit Association (maintaining qualifications for 501(c)(3) tax-exempt status, legally converting to IDIA DUNA upon reaching 100 governance members).

On-Chain Voting and Execution

Extending OpenZeppelin's `ERC20Votes` standard, the token enables holders to execute on-chain governance delegation. Utilizing the `IDIAGovernor.sol` contract and the `TimelockController` (which enforces a 48-hour execution delay), token holders govern the protocol's core decentralized parameters. This includes voting on the deployment of the localized 10% Community Grant Pools (regional War Chests managed via `IDIA_LocalizedPool.sol`), adjusting platform fee logic, and directing ecosystem treasury distributions.

To ensure the network is governed by its active participants rather than purely speculative capital, IDIA Governance Tokens are escrowed and distributed to data contributors numerically matched 1:1 with their earned Synapse Credit data yields.

7.3 Separation of Network Governance and Corporate Equity

To maintain strict compliance with United States securities regulations and establish clear legal boundaries for institutional investors, IDIA Data Inc. explicitly decouples network governance from corporate ownership.

1. No Corporate Equity or Shareholder Rights The IDIA Governance Token confers voting and administrative rights strictly within the DUNA. It explicitly does not represent corporate equity, stock, or ownership in IDIA Data Inc. Holding the IDIA Governance Token does not grant the holder traditional shareholder rights, voting power regarding corporate board appointments, or any legal claim to the equity valuation of the private corporation.

2. No Claim to Corporate Profits or Intellectual Property The IDIA Protocol separates the public-good governance layer from proprietary corporate infrastructure. While the DUNA controls the open-source ledger contracts and localized community grant pools, the core underlying algorithmic intellectual property—specifically the IDIA Synapse AI Engine—is expressly excluded from all DAO transfers and remains the sole, proprietary asset of IDIA Data Inc. Furthermore, the governance token provides no dividend claim or legal right to the 60% Platform Infrastructure revenue generated by enterprise Synapse Credit consumption; those funds remain strictly corporate operating revenue for IDIA Data Inc.

7.4 Synapse Credit Issuance, Consumption, and Restrictions

While the Governance Token manages protocol operations, Synapse Credits function strictly as internal, consumption-based API meters.

Issuance and Pricing: Enterprise buyers acquire Synapse Credits dynamically within *The IDIA Hub* dashboard by funding their treasury vaults via fiat gateways or USDC deposits. Synapse Credits are minted programmatically to the buyer's account balance at a fixed algorithmic peg of \$0.75 USD per credit.

Consumption and Expiration: Synapse Credits are strictly consumed via enterprise data extraction (e.g., executing a parameterized SQL query or an MCP agent context request).

- Credits are non-transferable; an enterprise buyer cannot sell, trade, or transfer their credit balance to another registered enterprise.
- To prevent the hoarding of internal utility meters and ensure continuous platform liquidity, Synapse Credits carry a 12-month expiration window. Unused credits expire 365 days from the date of purchase and are non-refundable, subject to the conditions outlined in the Master Service Agreement (S-3-C).

7.5 Dual-Distribution: USDC Settlement and Token Matching

To align immediate financial compensation with long-term network governance, the protocol employs a dual-distribution settlement architecture whenever a Synapse Credit is consumed.

- **Immediate Fiat Settlement (USDC):** The 30% Contributor Royalty Split is converted to USDC and routed instantaneously by the Synapse Engine to the non-custodial wallet of the Sovereign Node. This provides the user with immediate, liquid purchasing power.
- **Programmatic Governance Matching:** Simultaneously, the protocol matches the USDC royalty yield 1:1 numerically with IDIA Governance Tokens, distributed from the 30% Ecosystem / Treasury allocation pool. This ensures that users who generate the most verified "Ground Truth" for the network proportionally increase their administrative voting power within the DUNA over time.

7.6 Treasury Mechanics, Vesting, and Liquidity Disclosures

To prevent market manipulation and ensure the long-term stability of the governance asset, IDIA enforces strict, programmatically defined vesting schedules and multi-signature treasury controls.

- **Vesting Schedules and On-Chain Push Administration:** IDIA Governance Tokens allocated to the Team & Advisors (15%) and Early Investors (10%) cohorts are governed

by strict on-chain vesting schedules. Under the Early Investors Token Warrant structure, allocations are administered via `IDIAFundingRound.sol` and `IDIAVestingManager.sol` with no cliff period: 10% vests immediately upon the Vesting Commencement Date via `IDIAFundingRound.sol`, and the remaining 90% vests linearly across 72 equal monthly installments (6 years) via automated, batched on-chain push sequences from `IDIAVestingManager.sol`. Unvested balances remain subject to programmatic forfeiture (forfeit function) upon termination of alignment, ensuring early capital remains committed to the long-term stability of the protocol. This ensures that founding members and early capital are economically aligned with the long-term success of the protocol.

- **Liquidity and Market Operations:** Initial protocol liquidity (35% allocation) has been deployed to Automated Market Maker (AMM) pools (such as Uniswap on the Base network) to establish the initial routing mechanisms for the token. The liquidity pool tokens (LP Tokens) generated from these initial pairings are secured within the Gnosis Safe treasury to prevent premature liquidity extraction (rug-pull risk).

7.7 Smart Contract Architecture, Administrative Keys, and Upgrade Controls

The core IDIA smart-contract suite operates on the Base Layer-2 network (`0x6526F939D257E67896821c25B6C24Daa404a01FB`) and utilizes audited OpenZeppelin primitives governed by a Gnosis Safe multi-signature architecture. While the IDIA Protocol intellectual property and the **IDIA Synapse AI Engine** remain the sole, excluded property of IDIA Data Inc., the following on-chain contracts execute the public-good ledger and governance mechanics:

1. Core Smart Contract Registry

- **IDIA Governance Token (ERC-20):** Fixed 10,000,000,000 supply minted at deployment across five escrow vaults. Extends OpenZeppelin `ERC20Votes` (on-chain delegation and vote tracking), `ERC20Permit` (gasless approvals via EIP-2612), and `ERC20Burnable`. Owned by the Gnosis Safe, which executes `syncGovernanceState()` to emit governance pulse events directly to the *Life by IDIA* mobile client.
- **IDIAEscrow.sol (Multi-Sig Allocation Vaults):** Deployed five times (once per token allocation category: 35% Liquidity & Staking, 30% Ecosystem/Treasury, 15% Team & Advisors, 10% Early Investors, 10% Public Sale/Airdrop). Implements a lightweight 2-of-2 multi-sig protocol: the treasury wallet proposes distributions (`recipient, amount, reason`), and a registered approver managed by the Gnosis Safe must countersign before tokens release. Every distribution is permanently logged on-chain with timestamps.



- **IDIAGovernor.sol (On-Chain Governance):** OpenZeppelin Governor v2 calibrated for Base L2's ~2-second block time: **43,200 blocks (~1 day) voting delay**, **302,400 blocks (~7 days) voting period**, **4% quorum**, and a **zero proposal threshold**. Token holders must delegate votes (including self-delegation) to participate.
- **TimelockController (Execution Delay):** Sits between IDIAGovernor and protocol-critical actions, enforcing the mandatory **48-hour execution delay** specified in the Operating Agreement (60 seconds on testnet). The Governor holds PROPOSER_ROLE, EXECUTOR_ROLE is open (address(0) after delay expiration), and the Gnosis Safe holds DEFAULT_ADMIN_ROLE for emergency administration.
- **IDIARegistry.sol (Jurisdictional Location Registry):** Maps location identifier strings (formatted as "City_State_Country") to deployed regional pool addresses. A backend function calls getPoolByLocation() to route the 10% War Chest fee. Unregistered locations (address(0)) automatically fall back to the Global War Chest. Owned by IDIAPoolFactory to enable automated registration upon deployment.
- **IDIAPoolFactory.sol (Regional Pool Deployer):** Deploys IDIA_LocalizedPool instances and auto-registers them in IDIARegistry in a single atomic transaction while preventing duplicate jurisdictional deployments. Owned by the Gnosis Safe.
- **IDIA_LocalizedPool.sol (Regional Treasury Vault):** Autonomous vault holding the 10% localized fee allocation for a specific jurisdiction, utilizing SafeERC20 for secure token transfers and community grant execution.
- **IDIALiabilityReceipt.sol (Soulbound Data Purchase Receipt):** Non-transferable, non-burnable ERC-721 NFT (**ERC-5192 Soulbound standard**). Each minted token records the enterprise buyer's address, the contributing ACA consent hashes, purchase amount, Synapse receipt reference, and data bundle ID. Metadata is stored 100% on-chain as base64-encoded JSON within tokenURI (eliminating external IPFS dependencies). The treasury wallet holds MINTER_ROLE, and minting a receipt triggers the 1:1 IDIA Governance Token matching distribution to data contributors.

2. Key Control and Independent Security Reviews

There are no unilateral single-owner admin keys; all administrative functions require multi-party Gnosis Safe authorization and flow through the 48-hour TimelockController. All proprietary contract extensions (IDIARegistry, IDIA_LocalizedPool, and



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

IDIALiabilityReceipt) are scheduled for formal, independent third-party smart-contract penetration audits prior to broad national scaling.

7.8 Legal Review and Compliance Policy Statement

IDIA Data Inc. recognizes that the regulatory landscape surrounding digital assets and data privacy is continuously evolving.

- All IDIA marketing claims, token distribution mechanics, and governance frameworks are subject to continuous review by external legal counsel specializing in U.S. securities law, the Bank Secrecy Act (BSA), and global privacy frameworks (GDPR, CCPA).
- The distribution of the IDIA Governance Token is explicitly structured to avoid classification as an investment contract under the Howey Test.
- IDIA explicitly disclaims any financial guarantee regarding the secondary market price of the IDIA Governance Token. The token is engineered strictly for administrative utility within the DUNA, and all ecosystem participants must acknowledge these legal constraints prior to network interaction.



Section 8

DATA-AS-PERFORMANCE FRAMEWORK

To transition ambient digital exhaust into a compensated asset, the IDIA Protocol applies the operational mechanics of performance rights administration to the data economy. This framework requires absolute precision in tracking the lifecycle of a data asset from its initial registration to its commercial consumption.

8.1 Repertoire Registration and Cryptographic Attribution

The foundational requirement of a performance-based licensing model is the establishment of a verifiable, indisputable record of contribution. The IDIA Protocol achieves this through Sovereign Node registration, ensuring that every data asset is permanently mapped to its rightful contributor without exposing their underlying human identity.

1. Establishing the Verifiable Source Record

When a contributor connects a hardware source (such as native biometric sensors via *Life by IDIA* or a Point-of-Sale terminal via *IDIA Pay*), the client application initiates a formal registration event. The protocol logs the specific Originating Device Identifier, the exact schema of the telemetry stream being authorized (e.g., spatial metrics, inventory logs, or cadence patterns), and the cryptographic address of the contributor's Base Layer-2 non-custodial wallet.

2. Decentralized Identifier (DID) Attribution

To enforce edge-level isolation of Personally Identifiable Information (PII), the attribution record replaces legal names and government identifiers with a generated Decentralized Identifier (DID). This DID serves as the internal administrative account number. It guarantees that when the IDIA Synapse Engine routes a performance royalty, the capital is mathematically locked to the exact Sovereign Node that provisioned the hardware source, establishing an unbroken, verifiable chain of custody from the hardware edge to the settlement ledger.

8.2 The Licensing Ledger: Mapping Rights and Consent

Registration establishes the source of the data, but commercial utilization requires explicitly documented legal boundaries. The IDIA Protocol manages these boundaries through the active lifecycle of the Auditable Consent Artifact (ACA), which functions as a dynamic licensing ledger for every registered data stream.



1. Recording Authorized Purposes and Restrictions

During the registration of a data source, the contributor utilizes the *Life by IDIA* or *IDIA Pay* interface to configure granular consent parameters. The ACA records exactly how the data may be utilized. A contributor may authorize their data for "Quantitative Financial Analysis" while explicitly restricting it from "Insurance Underwriting" or "Biometric Artificial Intelligence Training." The ACA hardcodes these commercial restrictions into the data payload before it ever reaches *The IDIA Hub*.

2. Permitted Recipients and Temporal Constraints

The consent record dictates precisely who may ingest the data and for how long. The ACA defines whether the data is authorized for general marketplace aggregation or restricted to specific, verified enterprise buyers. Furthermore, it records the active consent status and the mandated Time-to-Live (TTL) parameters.

3. Enforcement via the Synapse Engine

The IDIA Synapse Engine utilizes this cryptographic licensing ledger to govern all enterprise access. If an enterprise buyer submits a query that violates the authorized purposes, restrictions, or permitted recipient parameters hardcoded into the ACA, the Synapse Engine automatically blocks the extraction. This ensures that the commercial exploitation of the data never exceeds the explicit, documented permissions granted by the Sovereign Node at the time of registration.

8.3 Qualifying Use: The Digital Performance Record

In the traditional music publishing model, a performance royalty is triggered by a measurable commercial event—a radio broadcast or a digital stream. Within the IDIA Protocol, data licensing operates on the exact same logic. A registered data asset generates yield only when a "Qualifying Commercial Use" is logged by the protocol.

The Measurable Commercial Event

A Qualifying Commercial Use occurs at the exact millisecond an enterprise buyer consumes a Synapse Credit to extract a data payload from *The IDIA Hub*. Whether the buyer executes a parameterized SQL query or an autonomous AI agent requests an MCP context injection, the successful delivery of that payload constitutes a digital performance.

Usage Record Generation

Every Qualifying Commercial Use generates an immutable usage record on the internal **ActivityLedger**. This record binds the enterprise buyer's execution event to the specific Auditable Consent Artifacts (ACAs) utilized in the payload. The usage record serves as the



definitive, auditable proof that the data was commercially deployed, triggering the immediate settlement pipeline.

8.4 Royalty Accounting and Deterministic Allocation

Once the usage record is generated, the IDIA Synapse Engine must programmatically calculate the exact payable amount owed to each individual contributor whose data was featured in the enterprise payload. The protocol eliminates subjective royalty accounting by applying a deterministic algorithmic allocation.

1. Applying the Allocation Rules

As established, the consumption of a \$0.75 Synapse Credit instantly isolates the 30% Contributor Royalty Split (\$0.225). Because a single macro-query may pull data from thousands of Sovereign Nodes simultaneously, this \$0.225 must be fractionalized across the entire contributing cohort.

2. The Calculation of the Payable Amount

To determine an individual contributor's exact payable amount, the Synapse AI Engine evaluates the specific data payload against its algorithmic weighting matrix (scoring the contribution from 0.1 to 1.0 based on fidelity, operational readiness, and temporal relevance).

- The engine calculates the total cumulative algorithmic weight of all ACAs utilized in the payload.
- It then divides the \$0.225 royalty pro-rata based on each node's precise fractional weight.
- The resulting calculation dictates the exact micro-transaction amount deposited into the contributor's non-custodial wallet, ensuring that compensation is directly mathematically correlated to the commercial quality and volume of the data provided.

8.5 Auditability, Adjustments, and Dispute Resolution

The administration of millions of fractional micro-transactions requires a transparent, highly resilient audit architecture. The IDIA Protocol maintains continuous, dual-entry records to ensure absolute financial integrity and to automate error correction.

1. Maintaining Licensing and Payout Records

Every node in the ecosystem maintains an automated, real-time audit trail.



- **For the Contributor:** *Life by IDIA* maintains the "Pattern of Life (PoL) Ledger," providing the user with a cryptographic receipt of every active license, every enterprise extraction, and every fractional USDC payout they have earned.
- **For the Protocol:** The backend `ProvenanceAuditLog` and the on-chain `IDIALiabilityReceipt` (minted to the enterprise buyer) preserve an immutable map linking the capital settlement back to the originating ACA hashes.

2. Automated Adjustments and Error Correction

In the event of a network latency failure, an interrupted backend function, or a disputed attribution, the protocol relies exclusively on cryptographic reconciliation rather than subjective human arbitration.

- If a Sovereign Node contests a missed payout, the protocol executes an automated reconciliation script comparing the user's localized ACA hash against the on-chain `IDIALiabilityReceipt` generated during the enterprise query.
- If the ledger confirms the user's data was successfully extracted but the corresponding Layer-2 USDC distribution failed (due to blockchain congestion or RPC node timeout), the protocol's automated error-correction mechanism flags the discrepancy and executes an immediate, retroactive settlement adjustment.
- By relying strictly on the cryptographic chain of custody, the protocol eliminates manual accounting disputes and ensures the systemic integrity of the performance framework.



Section 9

THE HUMAN RELIABILITY INDEX & SENSITIVE DATA

The Human Reliability Index (HRI) serves as the core diagnostic engine for the *Life Pro Series* (Pro, Pro+, and Pure Alpha). Because the HRI processes sensitive biological and behavioral telemetry, IDIA Data Inc. enforces strict definitional boundaries, access controls, and use-case restrictions to ensure compliance with global privacy and anti-discrimination frameworks.

9.1 Definitional Scope: What the HRI Measures (and What it Does Not)

To prevent regulatory misclassification and enterprise misuse, the IDIA Protocol explicitly defines the legal and operational parameters of the HRI.

What the HRI Is: The HRI is a real-time, individual-level diagnostic metric. Powered by the Cognitive Performance Module (CPM) and Occupational Performance Module (OPM), it measures immediate biological uptime, physical fatigue vectors, and operational readiness based on localized biometric telemetry. It functions strictly as a dynamic occupational safety gauge for high-consequence environments (e.g., ensuring a commercial pilot or logistics operator possesses the baseline biological readiness to safely complete a shift).

What the HRI is NOT:

- **Not a Medical Diagnosis:** The HRI does not diagnose, treat, or monitor clinical medical conditions, diseases, or chronic illnesses. It is entirely non-clinical.
- **Not an Absolute Guarantee:** It provides a predictive probability of operational stability; it is not an absolute, legally binding guarantee of future human performance or safety.
- **Not a Permanent Measure of Worth:** It is an assessment of real-time systemic readiness, not a permanent evaluation of a contributor's fundamental merit, intellect, or long-term employability, financial status, or access to capital advances.

9.2 Data Inputs and Affirmative Consent Requirements

The HRI is calculated utilizing specific, opt-in telemetry categories, primarily sourced through native OS biometric bridges (e.g., Apple HealthKit, Google Fit) and third-party wearables.

- **Data Categories:** Inputs include continuous Heart Rate Variability (HRV), resting heart rate, sleep duration baselines, and CPM mobility diagnostics (gait cadence, walking asymmetry, and step volume).
- **Consent Gating:** Processing this sensitive telemetry requires a dedicated, elevated Auditable Consent Artifact (ACA). The contributor must affirmatively opt-in to the *Life*

Pro series; the protocol will never passively scrape background biological data to generate an HRI score without explicit, cryptographically bound user authorization.

9.3 Prohibited Enterprise Uses and Anti-Discrimination Boundaries

IDIA Data Inc. actively mitigates the risk of "bio-redlining" — the discriminatory penalization of individuals based on algorithmic biological variances. Enterprise buyers must contractually agree to strict prohibited uses under the Master Service Agreement:

- **Automated Employment Termination:** The HRI may be used to verify safety readiness for a specific shift (e.g., temporarily grounding a fatigued driver), but it is strictly prohibited from being utilized as the sole, automated determinant for permanent termination, demotion, or hiring denial.
- **Insurance and Credit Denials:** The HRI cannot be utilized to deny an individual primary health insurance coverage, life insurance policies, or consumer credit. (Financial behavioral creditworthiness is explicitly relegated to the separate, non-biological *Trust Score*).

9.4 Validation, Hardware Uncertainty, and Ephemeral Processing

Institutional buyers must acknowledge the inherent uncertainty integrated into the HRI's algorithmic output.

- **Error Rates and Hardware Variance:** Because IDIA does not manufacture the underlying biometric sensors, the HRI is subject to the calibration errors, hardware degradation, and baseline variances of third-party OEM hardware (e.g., a loose Apple Watch strap returning anomalous HRV readings).
- **Ephemeral State:** To prevent stale data from negatively impacting a contributor, HRI scores are real-time, temporary outputs. While the raw, baseline telemetry (Tier-0 Sovereign Data) is persistently stored in secure cloud environments, the actual HRI diagnostic score is calculated dynamically in-memory and is not warehoused as a permanent, historical ledger of fatigue.

9.5 Access Controls, Hardware Airlocks, and User Challenges

The protocol enforces absolute zero-trust architecture regarding the ingestion of sensitive biological data.

- **Tier-0 Sovereign Data Isolation:** Raw, highly sensitive waveform data (such as raw ECG or granular HRV feeds) remains securely isolated at the edge or within hardware-secured execution environments (such as AWS Nitro Enclaves). IDIA corporate engineers possess zero access to unencrypted, identifiable Tier-0 biological records.
- **Dispute and Correction Mechanics:** Because the HRI is a real-time reflection of hardware ingestion, the protocol does not utilize manual customer-service overrides for "bad scores." If a Sovereign Node believes their HRI score is inaccurate due to a sensor glitch, the user controls the remediation: they can recalibrate their hardware, disconnect the specific OEM sensor feed, or utilize the *Life by IDIA* dashboard to instantaneously revoke the ACA governing the biometric stream, immediately halting any enterprise access to the disputed diagnostic.

9.6 Infinite Authentication and the Bio-Oracle Framework

Building directly upon the foundational bio-telemetry layers of the HRI, the IDIA Protocol deploys **Infinite Authentication** powered by the **Bio-Oracle** framework. Embedded inside the HRI architecture, the Bio-Oracle maintains continuous, uninterrupted cryptographic verification of the human operator.

By replacing static, episodic password logins with real-time biometric liveliness checks and continuous behavioral validation (such as gait cadence and device-interaction dynamics), Infinite Authentication eliminates the exposure windows exploited by synthetic impersonation and deepfake spoofing. State changes, verification handoffs, and telemetry provenance are cryptographically enforced and anchored via the HRI's Bio-Oracle, guaranteeing that every data stream and transaction within the ecosystem is backed by an active, uncompromised human presence.

9.7 The IDIA Trust Score: Behavioral Creditworthiness vs. Biological Uptime

While the Human Reliability Index (HRI) measures *biological* readiness and is strictly prohibited from financial underwriting, the **IDIA Trust Score** operates as a completely separate, non-biological engine that quantifies **Behavioral Creditworthiness and Prosocial Integrity** within the IDIA ecosystem.

- **Earning Social & Behavioral Capital:** Contributors earn points toward their Trust Score by verifying prosocial contributions ("Good Deeds") within the **Trust Circle**, validating community data accuracy, and demonstrating consistent, responsible financial and data habits within the ecosystem (such as settling merchant transactions on time, maintaining consistent telemetry uptime, and preserving sovereign wallet balances).
- **Internal Ecosystem Utility:** The Trust Score serves as a behavioral alternative to legacy credit bureaus, enabling high-integrity Sovereign Nodes to unlock lower-friction terms



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

and internal ecosystem advances based on verified Data Consistency and social capital rather than predatory debt history.

- **Visual Realization (The Sphere of Life):** Within the *Life by IDIA* application, a contributor's real-time Trust Score is visually represented by the color progression of their **Sphere of Life** interface—scaling across tiers from **White Pearl** (entry baseline) to **Vantablack** (highest verified prosocial and behavioral integrity).



Section 10

MARKET, COMPETITION, AND GO-TO-MARKET STRATEGY

A robust technical architecture is only valuable if it solves an urgent, funded enterprise problem. IDIA Data Inc. bypasses commoditized, low-margin advertising data markets to execute a highly targeted Go-To-Market (GTM) strategy focused on high-liability, mission-critical sectors.

10.1 First Buyer Persona and the Urgent Data Problem

The Buyer Persona: The Chief Risk Officer (CRO) and Chief Technology Officer (CTO) operating within regulated enterprise environments, legal tech, and frontier Artificial Intelligence development.

The Specific Problem: These executives face an existential crisis of "Ground Truth." Ingesting scraped, unverified web data to train AI models or underwrite risk introduces catastrophic legal liability (copyright infringement, privacy violations) and technical degradation (Model Collapse via synthetic AI Slop). They urgently require high-fidelity, legally indemnified, and cryptographically verified human telemetry, but possess no internal infrastructure to manage the millions of granular consent records required to procure it legally.

10.2 The Initial Vertical: Regional Public Infrastructure and Compliance

Rather than attempting a broad, unfocused national consumer launch, IDIA enters the market through regional public infrastructure and highly regulated operational compliance.

- **The Entry Point:** Mission-critical entities requiring immutable audit logging and FBI CJIS-compliant data environments (e.g., municipal infrastructure, missing persons databases).
- **Why It Is the Best Entry Point:** Securing procurement in a highly regulated, federally compliant environment forces the protocol to prove its absolute highest standard of security. Once the IDIA liability shield and cryptographic provenance are validated by law enforcement and federal infrastructure standards, downstream commercial adoption (such as logistics or retail) becomes frictionless.

Public Infrastructure & Compliance: The Ultimate Ground Truth

The ultimate validation of the Verified Truth Economy lies in its seamless integration with mission-critical public infrastructure and highly regulated government sectors. Beyond commercial enterprise deployment, the IDIA Protocol provides an immutable, cryptographically verifiable compliance framework designed for high-consequence public environments. By maintaining tamper-evident audit logging, zero-knowledge validation rails, and rigorous cryptographic provenance across state and municipal architectures, the network guarantees



absolute data integrity without sacrificing individual digital privacy. This institutional-grade reliability bridges the gap between decentralized digital sovereignty and public sector oversight, anchoring a trillion-dollar valuation model in secure, uncompromised public infrastructure.

10.3 Competitive Differentiation: The Consolidated Protocol

IDIA Data Inc. supersedes legacy data brokers by rendering their compliance models obsolete. Institutional buyers currently attempt to solve the data provenance crisis by piecing together fragmented vendors. IDIA consolidates this into a single, indemnified pipeline.

- **Versus Legacy Data Brokers (e.g., Experian, Acxiom):** Legacy brokers rely on passive, non-consented web scraping. They offer immense volume but massive regulatory liability. IDIA offers zero-PII, cryptographically consented ground truth backed by an enterprise liability shield.
- **Versus Consent Managers (e.g., OneTrust):** Consent managers help websites track cookie compliance, but they do not monetize the data or operate a commercial marketplace. IDIA integrates consent generation directly into the commercial settlement rail.
- **Versus Royalty Administrators:** Traditional administrators manage intellectual property (music, film) but lack the edge-computing architecture to process live physiological telemetry or operational metadata. IDIA applies rights-administration logic directly to live biometric and commercial data.

10.4 Enterprise Sales Cycle and Integration Burden

The Procurement Process: The enterprise sales cycle is direct and strictly gated. It requires the execution of the Master Service Agreement (S-3-C) and the successful completion of the T-1-P Technical Vetting Protocol. IDIA Sales Engineers audit the buyer's database architecture to ensure they are technically incapable of executing re-identification (the Mosaic Effect) before any data egress is authorized.

The Integration Burden: IDIA minimizes enterprise integration friction by delivering data in standardized, developer-native formats. Buyers are not required to adopt proprietary blockchain nodes. Data is delivered via low-latency REST APIs, secure WebSockets, parameterized SQL bundles, or the standardized Model Context Protocol (MCP) for autonomous AI agents.



10.5 Traction and Pipeline Separation

To maintain strict institutional transparency, IDIA Data Inc. explicitly demarcates recognized, contracted operational agreements from prospective discussions and uncontracted pipeline.

1. Signed Agreements and Active Technical Integration:

- **Zebra Technologies:** IDIA has executed an Independent Software Vendor (ISV) addendum (April 2026), formalizing enterprise hardware integration for Zebra TC58 devices across the IDIA Pay ecosystem.
- **J. Computer Solutions LLC (Project Aziz):** IDIA has established a Memorandum of Understanding (Oct 2026) to provide immutable auditability and CJIS-compliant ledger logging for missing persons data via *The IDIA Hub*.
- **DigiRAMP LLC:** Strategic partnership established for digital rights management, data validation, and intellectual property provenance services.

2. Prospective Pipeline and Active Discussions:

- **Federal Procurement Responses:** IDIA is engaged in joint strategic responses alongside prime contractors (Dfuse Technologies) for federal technology solicitations, including National Nuclear Security Administration (NNSA) compliance logging.

3. Paying Customers:

- The protocol is currently transitioning from closed beta into paid commercial piloting. Initial Synapse Credit consumption revenues will be recognized upon the official launch of the Louisville regional merchant rollout.

10.6 The Louisville Pilot Strategy and Success Criteria

The immediate Go-To-Market strategy is anchored by a hyper-local, high-density commercial pilot in Louisville, Kentucky.

The Strategy: IDIA will onboard a localized cohort of 10 to 15 paid "Founding Partner" commercial merchants onto the *IDIA Pay* Point-of-Sale architecture. Simultaneously, the *Life by IDIA* consumer application will be heavily marketed within this specific geographic radius to create a localized closed-loop data economy, generating verified commercial velocity and localized biometric telemetry.



Measurable Success Criteria for Series A Scaling: Before allocating capital toward broad national expansion, the Louisville Pilot must successfully validate the following key performance indicators (KPIs):

1. **Time to Onboard:** Reducing the friction of establishing a merchant Sovereign Node to under 48 hours.
2. **Consent Density:** Ensuring >95% of ingested commercial transactions successfully generate an Auditable Consent Artifact (ACA).
3. **Enterprise Conversion:** Successfully securing initial paid Synapse Credit consumption from external regional buyers querying the Louisville dataset.
4. **Settlement Accuracy:** Proving 100% cryptographic accuracy in the algorithmic weighting and instantaneous Base L2 USDC royalty distribution to the contributing cohort.

10.7 The Marketing Sequence: Post-Readiness Scaling

IDIA Data Inc. employs a milestone-gated marketing sequence. Broad commercial marketing capital is strictly withheld until product stability, legal compliance, and security readiness milestones—including independent smart-contract audits, SOC 2 compliance, and Phase 1 Money Transmitter Licenses (MTLs)—are officially secured. Once these gates are passed, the protocol scales through a three-phased sequence:

Phase 1: Hyper-Local Community Density (The Pilot Phase) Marketing initially bypasses traditional digital advertising in favor of grassroots, localized density. Focused entirely on the Louisville region, IDIA hosts educational town halls (addressing data surveillance and AI rights) to onboard individual Sovereign Nodes, while deploying direct-sales teams to onboard localized merchants onto *IDIA Pay*. The goal is to establish a closed-loop, verifiable data economy within a single geographic radius.

Phase 2: Account-Based Enterprise Sales (B2B) To enforce edge-level isolation of Personally Identifiable Information (PII), the attribution record replaces legal names and government identifiers with a generated Decentralized Identifier (DID). This DID serves as the internal administrative account number.

Phase 3: Developer Relations and Protocol Hegemony (Post-Series A) As the protocol achieves localized density and initial enterprise Annual Recurring Revenue (ARR), the marketing sequence targets the AI developer ecosystem. By integrating standard Model Context Protocol (MCP) endpoints and releasing SDKs for autonomous agent developers, IDIA transitions from a localized marketplace into a foundational utility—positioning *The IDIA Hub* as the default verification layer for the global agentic economy.



10.8 Acquisition and Retention Assumptions (Validation Gates)

To de-risk the protocol for Series A institutional capital, the Louisville Pilot is designed to scientifically validate several core unit-economic and behavioral assumptions before national scaling is initiated:

1. The "Zero-CAC" Consumer Acquisition Assumption

- **Hypothesis:** Because the IDIA Protocol transforms individuals into Sovereign Proprietors (enabling schedule C tax deductions and direct USDC data yields), consumer Customer Acquisition Cost (CAC) will approach zero through organic, tax-driven virality and merchant-led onboarding.
- **Validation Gate:** The pilot must demonstrate that localized users will actively register a Sovereign Node and generate an Auditable Consent Artifact (ACA) without requiring heavy direct-to-consumer ad spend.

2. The Merchant Retention Assumption

- **Hypothesis:** Retail and logistics merchants will remain locked into the *IDIA Pay* ecosystem because the platform offers 0% processing fees on native stablecoin transactions, while the Business Health Index (BHI) provides superior operational analytics compared to legacy POS systems.
- **Validation Gate:** The pilot must prove less than 5% voluntary merchant churn over the first two operating quarters, validating that the software utility and cost-savings outweigh the switching friction.

3. The Enterprise "Land and Expand" Assumption

- **Hypothesis:** Once an enterprise buyer successfully executes a query and experiences the cryptographic liability shield, their internal algorithmic systems (or autonomous agents) will programmatically increase their consumption of Synapse Credits month-over-month.
- **Validation Gate:** Net Revenue Retention (NRR) from initial enterprise cohorts must exceed 120%, proving that institutional buyers naturally scale their API metering usage once integrated into *The IDIA Hub*.

10.9 The Enterprise Go-To-Market (GTM) Bridge: From Pilot to Sovereign Utility

Beyond commercial logistics and municipal CJIS compliance, initial high-velocity Synapse Credit consumption bridging Year 1 revenue targets to institutional scale is driven across three specialized enterprise verticals:

1. **Legal & Civil Rights Enforcement (Empirical Damages Indexing):** National technology-litigation and civil rights law firms utilizing *The IDIA Hub* market clearing price (\$0.75 per Synapse Credit) as a standardized, empirical valuation index to calculate precise liquidated damages in mass-surveillance, unauthorized AI scraping, and digital property-tort class-action litigation.
2. **Federal & Critical National Infrastructure:** High-consequence federal agencies—explicitly targeting initiatives such as the **U.S. Department of Energy (DOE) Genesis mission** and National Nuclear Security Administration (NNSA) solicitations—requiring an immutable financial and operational validation layer, tamper-evident document provenance, and a persistent multi-agent security suite (*Crazy 8*).
3. **Hyperscale AI & Quantitative Finance:** Institutional quantitative desks, university research farms, and frontier AI labs procuring cryptographically verified, zero-PII data bundles and MCP context streams to inoculate foundation models against synthetic hallucination and Model Collapse.



Section 11

BUSINESS MODEL, FORECASTS, & ANGEL INVESTMENT

The transition of the IDIA Protocol from an operational pilot to a foundational national data utility requires disciplined capital deployment and transparent financial modeling.

11.1 Revenue Model Breakdown

IDIA Data Inc. generates corporate revenue across three distinct, highly scalable lines. (Note: The 30% Contributor Royalty Split is excluded from corporate revenue as it functions as a direct pass-through liability to Sovereign Nodes).

1. Sovereign Node Subscriptions (High-Margin SaaS)

- **Consumer Subscriptions:** Monthly recurring revenue from *Life Pro* (\$9.99), *Life Pro+* (\$49.99), and *Pure Alpha*(\$99.99).
- **Merchant Subscriptions:** Monthly recurring revenue from *IDIA Pay Pro* (\$49.99), providing the Business Health Index (BHI) and embedded operational intelligence.

2. Enterprise Licensing Fees (Annual Contracts)

- **Platform Access Licensing:** Recurring annual contracts providing enterprise buyers with Master Service Agreement execution, technical support, and access to *The IDIA Hub*. Tiers scale from Analyst (\$9,995/year) to Enterprise (\$49,995+/year).

3. Usage Fees (Metered Synapse Credit Consumption)

- **Platform Infrastructure Fee (60%):** The primary transaction engine. From every \$0.75 Synapse Credit consumed by an enterprise buyer, IDIA Data Inc. retains \$0.45 to fund cloud operations, data sanitization, and corporate profitability.

4. Baseline Unit Economics, Margins, and Metering Ratios

- **Synapse Credit Metering Ratio:** 1 Synapse Credit (\$0.75) = 1 Standard API Verification Call. 50 Synapse Credits (\$37.50) = 1 Soulbound Liability Token (IDIALiabilityReceipt.sol) Minting Event.
- **Consumer SaaS Unit Economics (*Life Pro*):** Estimated 3-Year Lifetime Value (LTV) of **\$450** against a **Near-Zero CAC** (driven by organic merchant onboarding and Schedule C tax-substantiation utility), yielding **>90% Gross Margin** (pure software delivery).



-
- **Enterprise Licensing Unit Economics (*The IDIA Hub*):** Target Annual Contract Value (ACV) of **\$85,000** against an estimated **\$12,000 CAC** (direct consultative sales & T-1-P engineering audit), yielding **~80% Gross Margin** after cloud and L2 settlement overhead.

11.2 Cost Structure and Operational Overhead

To support the protocol, IDIA Data Inc. incurs five primary categories of operational expenditure:

- **Infrastructure and Cloud Operations:** Costs associated with maintaining the AWS GovCloud data lakes, the LangGraph multi-agent orchestrator, edge-function routing, and RPC node providers for Base L2 connectivity.
- **Security and Cryptography:** Ongoing expenses for external penetration testing, *Crazy 8* agent maintenance, and smart-contract auditing.
- **Legal and Regulatory Compliance:** Capital allocated to multi-state Money Transmitter License (MTL) surety bonds, federal compliance counsel, and intellectual property defense.
- **Payments and Settlement:** Third-party gateway fees for fiat ingress (credit card/ACH processing) and corporate transaction fees.
- **Customer Success and Support:** Dedicated enterprise Sales Engineers for the T-1-P technical vetting process and merchant onboarding teams.

11.3 The 36-Month Operational Forecast

To ensure transparency, IDIA strictly separates confirmed, booked revenue from projected scaling hypotheses. *Note: The following forecast represents aggressive but modeled targets assuming full deployment of the Seed capital.*

Current Status (Month 0): Booked revenue is currently restricted to pre-launch test environments; official commercial Annual Recurring Revenue (ARR) recognition begins at the commencement of the Louisville Pilot.

Year 1 (Months 1–12): Pilot Validation and Regional Density

- **Focus:** Execution of the Louisville Pilot (10–15 paid merchants) and localized consumer density.



-
- **Targeted Revenue Hypothesis:** \$1.2M – \$2.5M. Primarily driven by early enterprise T-1-P adoptions querying the localized regional dataset and initial *Life Pro* consumer conversions.

Year 2 (Months 13–24): Multi-State Licensing and API Expansion

- **Focus:** Securing Phase 1 MTLs (CA, TX, NY, FL), enabling direct fiat rails and broader national merchant onboarding onto *IDIA Pay*.
- **Targeted Revenue Hypothesis:** \$8M – \$15M. Accelerated by the integration of autonomous AI agents utilizing the Model Context Protocol (MCP) bridge, drastically increasing Synapse Credit consumption velocity.

Year 3 (Months 25–36): Protocol Hegemony and Federal Procurement

- **Focus:** Successful deployment within federal critical infrastructure (e.g., Department of Energy/NNSA) and establishment as the default verification layer for quantitative finance.
- **Targeted Revenue Hypothesis:** \$40M – \$65M+. Shift toward massive, high-volume enterprise API metering and broad consumer SaaS adoption.

11.4 Angel & Seed Raise, Token Warrant Structure, Use of Proceeds, and Validation Milestones

IDIA Data Inc. is raising **\$10,000,000 in Seed Capital** structured via a **Simple Agreement for Future Equity (SAFE, Index Code: [FIN-SAFE-2026-B])** coupled with a **Token Warrant Agreement (SAFE Note Addendum)** at a **\$40,000,000 Pre-Money Valuation Cap** to fund an 18-to-24-month execution runway.

1. Structure of the Financing Instruments (SAFE + Token Warrant Addendum)

- **The SAFE ([FIN-SAFE-2026-B]):** Represents a contractual right to convert the Purchase Amount into future shares of IDIA Data Inc. Preferred Stock upon a qualifying Conversion Event (defined as a qualifying Equity Financing, Change of Control, or Initial Public Offering). Unlike a convertible debt instrument, the SAFE does not constitute a debt obligation, accrues zero interest, and confers no shareholder voting or dividend rights prior to conversion. Furthermore, the agreement incorporates a mandatory **Merit-Based Governance and Federal Compliance** covenant enforcing demographic neutrality and objective performance metrics to preserve corporate eligibility for prime federal contracting.



-
- **The Token Warrant Agreement (SAFE Note Addendum):** Executed alongside the SAFE, the Company grants the investor a non-transferable warrant to acquire a specified allocation of **IDIA Governance Tokens** under the *Early Investors* protocol category.
 - **Vesting and Cliff Schedule:** Token awards granted under the Warrant carry **No Cliff Period**. Exactly **10% of the total Award vests immediately** upon the Vesting Commencement Date. The **remaining 90% vests in 72 equal monthly installments** on the 1st of every month over a **6-year (72-month) total vesting period**, subject to continued alignment and compliance with Company policies.
 - **On-Chain Escrow and Automated Push Fulfillment:** Warrant allocations are secured and administered on-chain via **IDIAFundingRound.sol** (which processes the 10% immediate token release) and **IDIAVestingManager.sol** (which holds locked vesting balances under the *Early Investors* category). Vested tokens are distributed via automated, batched on-chain push sequences directly to the investor's wallet, eliminating manual claiming while providing an immutable, timestamped on-chain audit ledger.
 - **Forfeiture and Clawback Protections:** If an investor's relationship or contract alignment with the Company is formally terminated prior to completing the 72-month schedule, all unvested tokens held in **IDIAVestingManager.sol** are immediately and permanently forfeited back to the protocol treasury via the contract's native **forfeit** function. Additionally, all awards are governed by the Company's Financial Conflict of Interest (FCOI) Policy, under which a material breach may trigger a clawback of vested tokens as permitted by law.

2. Use of Proceeds (\$10,000,000 Allocation)

- **Technology & Core Engineering (40% | \$4,000,000):** Finalizing the LangGraph orchestrator, hardening the Vulture pipeline, and scaling the AWS GovCloud infrastructure.
- **Regulatory Compliance & Licensing (20% | \$2,000,000):** Securing required Phase 1 State Money Transmitter License (MTL) surety bonds, executing independent smart-contract security audits, and achieving formal SOC 2 Type II compliance.
- **Pilot Execution & Regional Acquisition (15% | \$1,500,000):** Funding the Louisville merchant rollout, validating the pilot, and executing the "Zero-CAC" organic consumer acquisition model.
- **Liquidity & Treasury Buffer (15% | \$1,500,000):** Capitalizing internal fiat settlement buffers and operational contingencies.



-
- **General Operations (10% | \$1,000,000):** Executive leadership, administrative overhead, and core enterprise sales teams.

3. Validation Milestones for Series A The Seed capital is deployed to achieve three explicit validation gates required for Series A scaling:

1. Completion of independent third-party smart-contract and SOC 2 security certifications.
2. Achieving a >95% Auditable Consent Artifact (ACA) generation rate across the Louisville pilot cohort.
3. Verified stress-test execution of the instantaneous Base Layer-2 USDC royalty settlement architecture under commercial load.

11.5 Risk Factors and Mitigation

Investors must acknowledge the major risks that could impede the achievement of these milestones:

- **Regulatory Friction:** Delays in state MTL approvals could temporarily restrict the direct fiat processing capabilities of *IDIA Pay*, forcing reliance on more expensive third-party payment facilitators.
- **Enterprise Integration Latency:** Large institutional buyers and federal agencies possess notoriously slow procurement cycles, potentially delaying the realization of Synapse Credit consumption revenue.
- **Hardware Dependency:** Changes to native OS privacy policies (e.g., Apple HealthKit updates) could temporarily restrict the flow of telemetry to the *Life by IDIA* node, requiring agile engineering updates to maintain HRI fidelity.

11.6 Corporate Equity (SAFE) vs. Governance Token Warrants

To eliminate any structural ambiguity regarding the Seed offering instruments:

- **Corporate Equity Rights (The SAFE):** The \$10,000,000 Simple Agreement for Future Equity ([FIN-SAFE-2026-B]) is a direct investment into the Delaware C-Corporation, IDIA Data Inc., representing a contractual right to receive future Preferred Stock upon a qualifying Conversion Event. Upon conversion into capital stock, holders receive a claim to the corporate balance sheet, proprietary intellectual property (the IDIA Synapse Engine), and the 60% Platform Infrastructure revenues. Until conversion, the SAFE confers no shareholder voting or dividend rights.



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

- **Network Governance Rights (The Token Warrant Addendum):** The accompanying Token Warrant Agreement is a distinct contractual addendum granting the right to receive IDIA Governance Tokens under a 6-year (72-month) vesting schedule. Until the formal exercise or vesting release of the Warrant, the holder possesses no rights as a holder of the Company's capital stock. Once vested and pushed via `IDIAFundingRound.sol` and `IDIAVestingManager.sol`, those tokens confer administrative voting power strictly within the Decentralized Unincorporated Nonprofit Association (DUNA) and carry zero equity or dividend claims in IDIA Data Inc.



Section 12

LEGAL, REGULATOR, AND GOVERNANCE DISCLOSURES

12.1 Statutory Privacy Frameworks and Jurisdictional Alignment

The IDIA Protocol is architected to operate in strict conformity with evolving global data protection regimes, including the European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA/CPRA), and comprehensive state-level privacy statutes across the United States (e.g., Virginia VCDPA, Colorado CPA).

- **Lawful Basis and Affirmative Consent:** In compliance with GDPR Article 6 and CPRA consent mandates, data ingestion is gated behind affirmative, unambiguous, and cryptographically verified opt-in actions recorded within the Auditable Consent Artifact (ACA). The protocol rejects passive, ambient, or bundled pre-checked consent mechanisms.
- **Edge-Level Decoupling vs. Pseudonymization:** Under GDPR Article 4(5), pseudonymized data remains subject to regulatory oversight if re-identification is feasible. IDIA mitigates statutory liability by decoupling Direct Identifiers (PII) at the device hardware enclave before network transmission, ensuring that the commercial data lake operates exclusively on mathematically sanitized, zero-PII records bound to ephemeral transaction hashes.
- **The Right to Erasure and Revocation:** In alignment with GDPR Article 17 ("Right to be Forgotten") and CPRA deletion rights, a contributor's revocation of an ACA instantly halts downstream commercial routing across *The IDIA Hub* and triggers automated Time-to-Live (TTL) deletion procedures across enterprise-licensed vaults.

12.2 Biometric Telemetry and Sensitive Data Regulations

Biometric data processing is subject to heightened legal scrutiny under state frameworks such as the Illinois Biometric Information Privacy Act (BIPA, 740 ILCS 14/), Texas Capture or Use of Biometric Identifier Act (CUBI), and Washington State biometric privacy legislation.

- **Affirmative Written Release:** Prior to the activation of the Cognitive Performance Module (CPM) or any biological sensor bridge within *Life by IDIA*, contributors execute a standalone, express biometric consent agreement defining the specific metrics captured, the exact commercial licensing scope, and the retention schedule.
- **Non-Storage of Raw Templates:** IDIA does not capture, store, or warehouse facial geometry, retinal scans, or raw fingerprint templates. Telemetry ingested consists strictly

of physiological motion and baseline autonomic trends (e.g., gait cadence, walking asymmetry, and continuous heart rate variability).

- **Ephemeral Diagnostic Processing:** To insulate the protocol from BIPA exposure, derived diagnostics generated by the Human Reliability Index (HRI) are calculated ephemerally in-memory by the IDIA Synapse Engine to resolve real-time queries. The resulting HRI score is not warehoused as a permanent, discoverable individual ledger, completely preventing the creation of long-term biological profiles.

12.3 Financial Services, Banking Integration, and Money Transmission

IDIA Data Inc. functions strictly as an administrative technology provider and commercial data licensing clearinghouse. It is neither a chartered banking institution, an insured depository entity, nor a licensed money transmitter under federal or state statutes.

- **Fiat Processing and Banking Rails:** All fiat transactions, including enterprise subscription billing and credit card processing for *The IDIA Hub* and *IDIA Pay*, are executed exclusively through third-party payment processors, licensed merchant acquirers, and Banking-as-a-Service (BaaS) partners. These regulated financial institutions maintain direct responsibility for compliance with the Bank Secrecy Act (BSA), anti-money laundering (AML) controls, and Customer Due Diligence (CDD) mandates.
- **Money Transmitter Licensing (MTL) Boundaries:** Direct transmission of customer funds is strictly circumscribed. Where state statutory thresholds deem the programmatic routing of commercial data licensing revenues to constitute regulated money transmission, direct fiat remittance is disabled pending the final approval and capitalization of IDIA's Phase 1 State Money Transmitter Licenses (CA, TX, NY, FL) and the posting of required surety bonds.
- **Non-Custodial Contributor Settlement:** Contributor royalty distributions are settled via Base Layer-2 smart contracts delivering USDC directly to the contributor's non-custodial wallet. IDIA Data Inc. maintains zero custodial possession, control, or unilateral withdrawal authority over contributor digital asset private keys.

12.4 Digital Asset Characterization and Securities Safe Harbors

The digital assets operating within the IDIA ecosystem are legally and functionally distinct, structured to operate in compliance with federal securities laws, SEC regulatory guidance, and the framework established under *SEC v. W.J. Howey Co.*

- **Synapse Credits:** Synapse Credits are internal, fixed-value (\$0.75 USD) consumable enterprise access units. They are non-transferable, non-refundable, cannot be traded on

secondary markets, and confer zero economic yield, ownership, or voting authority. They function purely as a technical utility metering API calls and Model Context Protocol (MCP) data consumption.

- **USDC Distribution:** Contributor performance royalties are distributed in USDC, a regulated, fiat-collateralized payment stablecoin utilized solely as a commercial medium of exchange for delivered data performance.
- **IDIA Governance Token:** Minted on the Base Layer-2 network (Supply: 10,000,000,000 IDIA; Contract: 0x6526F939D257E67896821c25B6C24Daa404a01FB), the IDIA token functions exclusively as an administrative voting instrument for the Wyoming Decentralized Unincorporated Nonprofit Association (IDIA DUNA). The token does not represent equity, stock, debt, or an investment contract in IDIA Data Inc. It carries no rights to corporate dividends, corporate liquidation preferences, or corporate intellectual property.
- **Delaware Series LLC Capitalization (\$SITs and Series I Preferred):** The Series I Telemetry Units (\$SITs) and Series I Perpetual Preferred Units issued by IDIA Indemnity Reserve, LLC are formal security derivatives offered exclusively to accredited institutional investors under statutory exemptions, including Regulation D, Rule 506(c) under the Securities Act of 1933, and applicable offshore regulatory regimes.

12.5 AI Governance, Foundation Model Ingestion, and Downstream Restrictions

To mitigate enterprise liability surrounding artificial intelligence development, data licensing agreements executed on *The IDIA Hub* enforce strict covenants governing downstream algorithmic ingestion:

- **Anti-Re-identification and the Mosaic Prohibition:** Enterprise buyers and AI developers executing Master Service Agreements (S-3-C) are contractually and technically prohibited from attempting to reverse-engineer, de-anonymize, or correlate IDIA pseudonymized datasets with external identity records (the Mosaic Effect).
- **Permitted Model Ingestion:** Licensed Data Assets may be utilized for machine learning training, algorithmic optimization, and quantitative backtesting solely within the parameters specified by the originating Auditable Consent Artifact (ACA).
- **Algorithmic Deletion Covenants:** In the event an enterprise buyer ingests data streams where consent is subsequently revoked, the buyer is contractually bound to purge the corresponding telemetry weights from active training caches and comply with verification audits administered by IDIA Data Inc.

12.6 Intellectual Property Boundaries and Asset Segregation

The IDIA ecosystem maintains a strict, unbreachable legal firewall between corporate intellectual property, decentralized network governance, and contributor data rights:

- **Proprietary Corporate Architecture:** All proprietary source code, software architectures, patent filings, trade secrets, edge-routing functions, valuation algorithms, and the core analytical engine—specifically the **IDIA Synapse AI Engine**, the **Human Reliability Index (HRI)** scoring codex, and the **Business Health Index (BHI)**—are and remain the exclusive, 100% owned intellectual property of IDIA Data Inc. Neither the DAO, the DUNA, nor any ecosystem participant holds any claim, license, or right of ownership over these corporate assets.
- **Decentralized Open-Source Governance:** The DUNA maintains authority solely over the public-good Layer-2 smart contract interfaces (`IDIAGovernor.sol`, `IDIARegistry.sol`, and the localized `IDIA_LocalizedPool.sol` regional vaults).
- **Administrative Agency Over Contributor Data:** Acknowledging that raw public facts and machine exhaust remain inherently uncopyrightable, contributors retain their original data rights and grant a defined, revocable administrative licensing agency. This empowers IDIA Data Inc. to act exclusively as their commercial licensing agent to package, monetize, and distribute zero-PII Licensed Data Assets.

12.7 Contractual Enforcement, Limited Power of Attorney, and Remedies

To protect the integrity of the data ecosystem and enforce enterprise compliance, Sovereign Nodes grant IDIA Data Inc. a specifically bounded Limited Power of Attorney (LPOA) upon source registration.

- **Scope of Legal Standing:** The LPOA is strictly limited to the administration, commercial licensing, billing, collection, and contractual enforcement of data rights granted through native IDIA interfaces. It empowers IDIA Data Inc. to negotiate enterprise Master Service Agreements, collect licensing fees, and initiate legal proceedings against enterprise buyers that violate license boundaries, fail to execute mandatory data deletions, or attempt unauthorized re-identification.
- **Liquidated Damages and Revocation of Defense:** Any enterprise buyer that breaches the non-re-identification covenant or sub-licenses IDIA data assets without authorization automatically forfeits all protections under the IDIA Liability Shield, triggers immediate cancellation of their soulbound `IDIALiabilityReceipt`, and becomes subject to contractual liquidated damages and injunctive relief.



- **No General Representation:** The LPOA does not constitute a general legal representation or an affirmative duty for IDIA Data Inc. to monitor the open web or pursue external third-party bad actors for unconsented scraping occurring outside the boundaries of the IDIA Protocol.

12.8 Document Harmonization, Dispute Resolution, and Governing Law

To ensure absolute operational and legal consistency across all touchpoints, the terms and disclosures set forth in this White Paper are systematically harmonized with IDIA Data Inc.'s operative legal instruments: the Consumer Terms of Service, the Merchant Services Agreement, the Data Processing Addendum (DPA), the Master Service Agreement (Form S-3-C), and the Statements of Designation of IDIA Indemnity Reserve, LLC.

- **Governing Law:** All corporate operations, enterprise licensing agreements, and platform terms are governed by and construed in accordance with the laws of the State of Delaware, without regard to conflict of law principles.
- **Institutional Arbitration:** Any dispute, controversy, or claim arising out of or relating to commercial licensing, protocol operation, or data distribution shall be settled by binding institutional arbitration administered by the American Arbitration Association (AAA) or JAMS in accordance with their Commercial Arbitration Rules, with proceedings conducted in Wilmington, Delaware.
- **Document Hierarchy:** In the event of any operational or structural ambiguity between this descriptive White Paper and executed commercial contracts, the provisions of the formal Master Service Agreement, executed Data Processing Addenda, and Corporate Charters shall strictly govern and supersede this document.

Section 13

MACROECONOMIC & SOCIETAL IMPLICATIONS

The transition to the IDIA Protocol represents a structural shift comparable to the most significant financial inflections of the last century.

13.1 The Deflationary Hedge (The "Reverse Nixon Shock")

In 1971, President Richard Nixon unilaterally decoupled the U.S. Dollar from the Gold Standard to resolve a crippling liquidity crisis, moving the global economy from a standard backed by scarce physical metal to a fiat standard backed by debt expansion.

In 2026, the global economy faces the inverse crisis: "AI Slop" and autonomous synthetic production are driving the marginal cost of digital labor and unverified information toward zero, triggering a severe **Deflationary Shock**. The IDIA Protocol executes a **"Reverse Nixon Shock"** by recoupling economic value to an irreproducible, scarce resource: **Verified Human Truth**. Just as petroleum became the implicit backing of the post-1971 fiat dollar (the Petrodollar), cryptographically verified human telemetry becomes the foundational backing of the algorithmic economy (the **Data-Dollar**). The Universal Basic Asset (UBA) preserves consumer purchasing power through continuous data royalties, preventing deflationary collapse by keeping human participation economically solvent.

13.2 Capital Efficiency (The "Ranieri Moment" for Human Reliability)

In 1977, Lewis Ranieri and Salomon Brothers pioneered the Mortgage-Backed Security (MBS), transforming static, illiquid local mortgages trapped on bank balance sheets into liquid global assets.

Today, an individual's daily operational reliability, biological uptime, and behavioral integrity represent trillions of dollars in **"Dead Capital"**—invisible, unverified, and illiquid signals that generate zero yield for the operator. The IDIA Protocol executes a **"Ranieri Moment" for Human Reliability**, standardizing consented operational telemetry into liquid, institutionally licensable data streams and **Series I Telemetry Units (\$SITs)**. Just as the MBS unlocked the capital value of physical real estate, the IDIA Protocol unlocks the economic value of human operational readiness without reducing the human being to a debt instrument.

13.3 The Sovereign Flip (The End of Digital Feudalism)

Under the "Digital Feudalism" of Web 2.0, individuals generated valuable behavioral exhaust for free while centralized technology oligarchs passively harvested, packaged, and monetized that telemetry. The IDIA Protocol establishes the **Sovereign Node** as the *Magna Carta* of the Agentic Age—transitioning individuals and small businesses from uncompensated digital subjects into

direct royalty recipients and voting DUNA participants governing the validation layer of the AI economy.

13.4 The Merit Alignment (Empirical Infrastructure for the Competence State)

As public and private institutions increasingly seek to replace bureaucratic credentialism (static, decades-old academic degrees) with objective merit and operational competence, they lack an empirical, real-time verification standard. A static PDF resume cannot prove cognitive readiness in a high-consequence environment today.

The **Occupational Performance Module (OPM)** within *Life by IDIA* provides the empirical infrastructure for a consent-based meritocracy. Rather than relying on subjective credentials or political patronage, operators in mission-critical roles can consensually present their real-time HRI readiness verification—demonstrating current cognitive endurance, reaction stability, and biological uptime.

13.5 Addressing "Bio-Redlining" (Occupational Safety vs. Discrimination)

Critics rightly warn against the danger of a "Biological Caste System" where algorithmic bias disqualifies capable candidates. IDIA structurally prevents bio-redlining through two strict mechanisms:

1. **Occupational Safety Framing:** Preventing a surgeon or commercial transport driver suffering from acute sleep deprivation from operating is not discriminatory profiling; it is empirical public safety.
2. **Ephemeral, Role-Matched Diagnostics:** Because HRI scores are strictly ephemeral (never warehoused as a permanent historical flaw) and contractually barred from automated firing or credit/insurance denials (Section 9.3), the OPM matches real-time biological readiness to immediate task safety rather than penalizing individuals for baseline genetic variance.



ANNEX I: QUANTITATIVE FINANCIAL MODEL

The following quantitative models outline the fundamental revenue engines, unit economics, and long-term projections underpinning the IDIA ecosystem.

Product Pricing Matrix (The Revenue Engine)

1. IDIA Pay (SMB FinTech) Strategy: "Land and Expand" via 0% Fees for Sovereign Users.

- Transaction Fees (On-Us/IDIA-USD): 0.00% (Loss Leader for Adoption)
- Transaction Fees (Off-Us/Legacy Card): 2.5% + \$0.10 (Competitive Market Rate)
- SaaS Subscription (Pay Pro): \$49.99/month
 - Includes: Business Health Index (BHI), Staff Fatigue Monitoring, Embedded Payroll.
 - Target: Merchants with >\$20k Monthly Volume.

2. Life by IDIA (Consumer/Workforce SaaS) Strategy: Freemium Model converting "Users" to "Prosumers."

- Life (Free): Basic Wallet, Trust Score, Passive Data Yields.
- Life Pro (Occupational Safety): \$9.99/month
 - Includes: HRI Dashboard, AI Feedback.
- Life Pro+ (Cognitive Readiness): \$49.99/month
 - Includes: Readiness Alerts, and Instrumentality Tooling.
- Pure Alpha (Executive Optimization): \$99.99/month
 - Includes: Clinical-Grade Bio-Telemetry, Private Wealth Dashboard, Priority Support.

3. The IDIA Hub (Enterprise Data & AI) Strategy: Tiered Access + Metered Consumption (API).

- Analyst Tier: \$9,995/year (Single Seat, Standard Datasets)
- Professional Tier: \$24,995/year (Team Access, Real-Time Feeds)
- Enterprise Tier: \$49,995+/year (Custom Integrations, Full Liability Shield)



- Synapse Credits (API Metering): \$0.75 per Credit
 - ◉ Usage: 1 Credit = 1 Standard Verification Call. 50 Credits = 1 Liability Token Minting.

4. Unit Economics & Margins

- Consumer LTV (Life Pro): \$450 (3-Year Horizon)
 - ◉ CAC: Near Zero (Viral/Tax-Driven Adoption)
 - ◉ Margin: >90% (Software Only)
- Enterprise Contract Value (ACV): \$85,000 + CAC: \$12,000 (Direct Sales)
 - ◉ Margin: ~80% (Infrastructure Costs)

Dual-Scenario Forecasting Methodology: Current Baseline vs. Cultural Agentic Saturation

Because the global transition toward autonomous artificial intelligence (the "Agentic Economy") is occurring along a non-linear adoption curve, IDIA Data Inc. evaluates its 10-year financial trajectory across two distinct velocity models. The divergence between these two projections is not a difference in product architecture, but a function of **external market velocity and autonomous agent saturation**:

1. **The "Kilocorn" Systemic Standard Model (Cultural & Macroeconomic Agentic Saturation):** Models the ceiling scenario in which cultural, commercial, and regulatory expectations of the Agentic Economy fully materialize. In this environment, autonomous AI agents rapidly supersede manual human workflows across global finance, supply chains, and risk underwriting. Because unverified agentic execution faces existential "Model Collapse" and uncapped tort liability, cryptographic human provenance and the IDIA Liability Shield become a mandatory systemic standard—positioning the protocol as a global monetary and clearing utility on par with a Systemically Important Financial Institution (SIFI).
2. **The Conservative Baseline Model (Current Empirical Agentic Adoption):** Models the foundational floor scenario, strictly constrained by current, observable enterprise AI adoption rates, standard B2B procurement cycles, and measured regulatory rollout. This model projects growth driven exclusively by traditional consultative enterprise sales, deliberate Model Context Protocol (MCP) developer integration, localized V-SaaS merchant expansion, and multi-year federal contracting (directly aligning with the 36-Month Operational Forecast established in Section 11.3).



Scenario A: The "Kilocorn" P&L Projection (10-Year Horizon — Cultural Agentic Saturation)

This model assumes the rapid cultural and regulatory transition from "Protocol Adoption" to mandatory "Systemic Standard," where autonomous AI agents require continuous, microsecond ground-truth verification and programmatic liability shielding across global commerce

Metric	Year 1 (The Protocol)	Year 3 (The Adoption)	Year 5 (The Standard)	Year 10 (The Hegemony)
Total Revenue	\$12.5 Million	\$4.2 Billion	\$68.5 Billion	\$450 Billion
-- Oracle Fees	\$500k	\$1.8B	\$25.0B	\$180B
-- Securitization Fees	\$0	\$1.5B	\$28.5B	\$150B
-- Collateral Monitor	\$2.0M	\$800M	\$12.0B	\$85B
Gross Profit	\$7.5M	\$3.4 Billion	\$58.0 Billion	\$385 Billion
EBITDA	(\$8.0M)	\$2.5 Billion	\$45.0 Billion	\$310 Billion
Valuation (Multiple)	\$150M (Seed)	\$50 Billion	\$1 Trillion	\$6.2 Trillion

Note: Year 10 Valuation assumes IDIA functions as a Systemically Important Financial Institution (SIFI), valued as a global monetary utility (Visa x Moody's x Federal Reserve).

Bridging the Horizon: From Systemic Ceiling to Empirical Baseline

While the Kilocorn projection illustrates the upper-bound macroeconomic capture if cultural expectations of ubiquitous agentic commerce accelerate exponentially, institutional underwriting requires a sober baseline anchored in **present-day adoption friction**.

In the current market environment, enterprise Chief Risk Officers and federal agencies integrate autonomous AI frameworks cautiously — gated by legacy IT infrastructure, multi-quarter compliance reviews (such as the T-1-P Technical Vetting Protocol), and phased state regulatory licensing. **Scenario B (The Conservative P&L Projection)** strips out hyper-accelerated macroeconomic assumptions and models IDIA Data Inc. strictly on **current agentic adoption velocity** and traditional B2B/SaaS unit economics.

Directly extending the Year 3 operational target outlined in Section 11.3 (\$40M–\$65M+), this baseline model demonstrates that even if global agentic adoption progresses only at today's measured, empirical pace, the Double-Helix revenue engine still scales into a highly profitable, multi-billion-dollar institutional infrastructure provider (\$4.85 Billion in Year 10 revenue at a 70% EBITDA margin) — protecting investor downside while preserving full exposure to the Kilocorn upside.



IDIA Data Inc. | IDIA DAO LLC | IDIA Indemnity Treasury LLC

Originally Drafted: Saturday, January 17, 2026

Updated Last: Wednesday, October 14, 2026

Scenario B: The Conservative P&L Projection (10-Year Horizon — Current Agentic Adoption Baseline)

Fiscal Year (FY)	Total Revenue	Total Operating Expenses	EBITDA	EBITDA Margin	Key Drivers & Phase
FY2028 (Y3)	\$64,543,685	\$9,893,725 (15.3%)	\$54,004,524	83.7%	CSV Validated Truth. Post-Pilot, Series A Secured, Highly Efficient MVP Operations.
FY2029 (Y4)	\$155,500,000	\$62,200,000 (40%)	\$93,300,000	60.0%	Blitz Phase: Marketing spend doubles to 40% to fuel customer acquisition and M&A integration.
FY2030 (Y5)	\$342,100,000	\$136,840,000 (40%)	\$205,260,000	60.0%	Marketing Blitz Continues, API Adoption Spikes, Angelic Product Dev Accelerates.
FY2031 (Y6)	\$684,200,000	\$205,260,000 (30%)	\$478,940,000	70.0%	Pivot to Scale: OpEx stabilizes to 30%. Federal Capture gains major traction.
FY2032 (Y7)	\$1,231,500,000	\$369,450,000 (30%)	\$862,050,000	70.0%	Significant API Revenue, Angelic Hardware Launch, Major V-SaaS Integrations.
FY2033 (Y8)	\$2,093,550,000	\$628,065,000 (30%)	\$1,465,485,000	70.0%	Dominant API Market Share, Angelic Reaches Scale, First Major Federal IDIQ Wins.
FY2034 (Y9)	\$3,349,600,000	\$1,004,880,000 (30%)	\$2,344,720,000	70.0%	Ecosystem Network Effects Fully Realized, Infrastructure Provider Status.
FY2035 (Y10)	\$4,850,000,000	\$1,455,000,000 (30%)	\$3,395,000,000	70.0%	Target Achieved. Market Leader Across Pillars, Preparing for Potential IPO.

CONCLUSION

The IDIA Protocol is replacing the Mortgage-Backed Standard with the Data-Backed Standard, we obsolete the concept of "Debt" and replace it with Sovereign Node participation. In this new economy, your value is the Truth you verify.

IDIA DATA INC. A good IDIA can change the world.