Federated AML Investigation

Cross-Bank Money Laundering Detection Without Sharing Raw Customer Data

Shaun Geer, Track 1, TechEx Intelligent Enterprise Solutions Hackathon, May 11 to 19, 2026

https://github.com/Airwhale/federated_silo_agent

Cross-Bank Laundering Is Invisible to Any Single Bank

Structuring rings, layering chains, and smurfing networks span institutions, yet each bank sees only it's own narrow slice of the picture.

The Blind Spot

No single bank holds enough signal to identify a multi-institution laundering scheme in progress.

314(b) Exists, But Stalls

Section 314(b) permits voluntary cross-bank sharing, yet remains underutilized because it's implementation is slow, manual, legally uncomfortable, and paper-driven.

Our Answer

We automate 314(b) collaboration into a governed, auditable, privacy-preserving federated workflow.

Four Frictions That Kill Cross-Bank Collaboration with 314(b)

⚖️ Legal Risk Aversion

If a bank reveals information they should not, creates legal exposure: Our system prevents this.

🏗️ No Standard Infrastructure

Every cross-bank request is ad hoc and paper-driven.

🔒 Privacy-Lawsuit Fear

If anonymization fails, the disclosing bank is named in the suit.

🏦 Competitive Paranoia

Banks fear sharing signals benefits a rival more than themselves.

Our Solution: A Governed Federation Layer

> LLMs are finally good enough to mediate §314(b) requests; OpenDP made Differential Privacy production-ready; the legal climate softened in 2023 around safe harbors. That's why this exists in 2026 and not 2018.

Peer banks respond with approved, privacy-preserving statistical signals only, no raw records cross boundaries. Federation agents combine signals into graph patterns, sanctions context, SAR evidence, and audit findings, delivering a result investigators and regulators can trust.

Security and Privacy by Design

Data Stays Local

No raw customer names, accounts, or transactions ever cross bank boundaries.

Lobster Trap

Every inter-agent message is checked against AML policy before reaching any model.

Cryptographic Integrity

Digital signatures, replay protection, and route approvals verify every message.

Differential Privacy

Aggregate statistics are noise-calibrated; every decision leaves a full audit trail.

Three AML Patterns We Model

Our demo tests three common cross-bank money laundering patterns. Each is hard for one bank to see alone, but clearer when banks share privacy-preserving signals.

Structuring Ring

A group splits large suspicious activity into many smaller transactions across multiple banks. Each bank sees only small pieces, but the federation detects the repeated pattern across institutions.

Layering Chain

Money moves through several linked entities and banks to make the source harder to trace. The system looks for chained movement patterns using aggregates, not raw transaction records.

Sanctions Evasion

A suspicious entity is connected to sanctions or politically exposed person risk through hash-only screening. The system flags the risk without revealing raw names or watchlist details.

The system detects cross-bank AML patterns while keeping customer identities and raw transactions inside each bank.

Three Attacks We Model

🧠 Prompt Manipulation

Attacker tricks an LLM into ignoring rules or revealing customer names.

Blocked by: Lobster Trap pre-model scanning.

📨 Fake or Altered Messages

Unsigned, replayed, or rerouted messages injected into the federation.

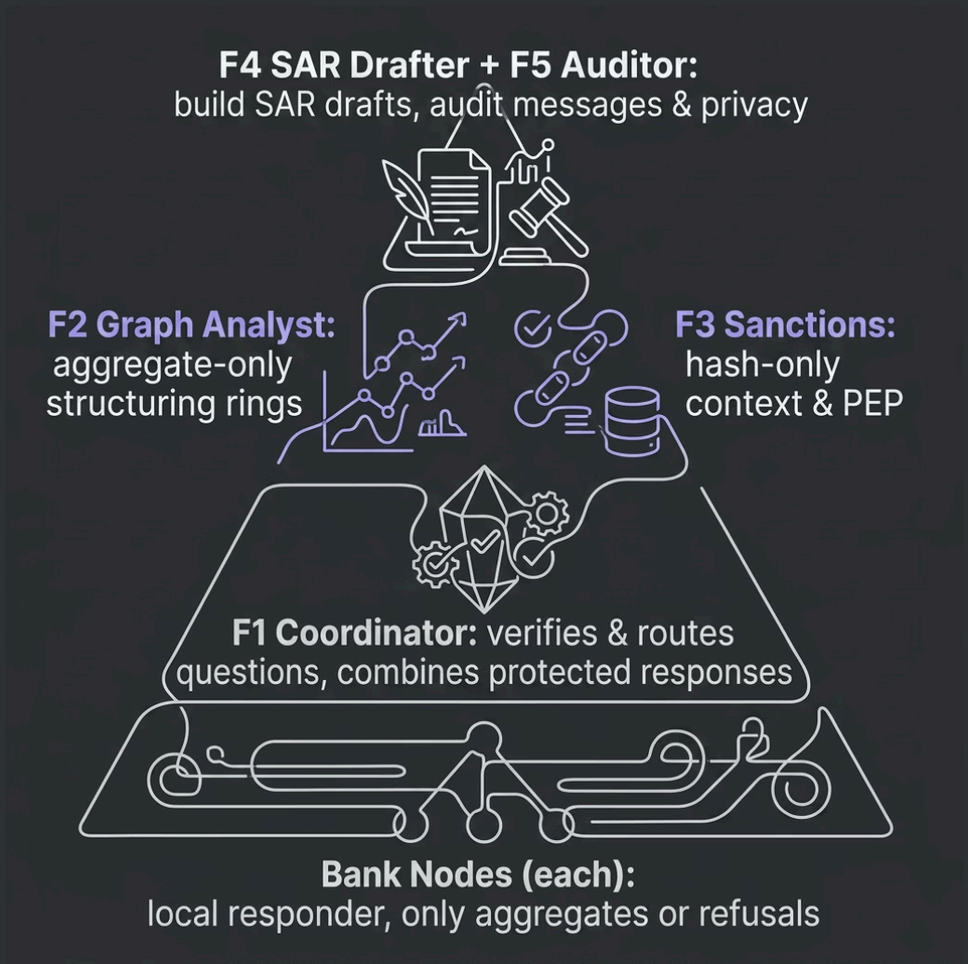
Blocked by: Cryptographic signatures from vetted allowlists, one-time IDs, and expiration checks.

🗂️ Private Data Overreach

Requests for raw transactions or repeated summary queries to re-identify individuals.

Blocked by: Local silo policy and privacy-budget enforcement.

High-Level Architecture



Federation Nodes

1	2
F1 Coordinator Verifies investigator requests, routes approved questions to banks holding raw data	**F2 Graph Analyst** Detects structuring rings and layering chains using aggregate-only data.
3	**4**
F3 Sanctions Screener Compares hash tokens coming out of investigation flow to detect sanctioned or politically exposed persons	**F4 SAR Drafter + F5 Auditor** Builds regulator-ready SAR drafts; audits message flow, refusals, and privacy-budget use.

Data Protections Built Into the System

Local Silos + Typed Refusals

Raw data never leaves; banks can safely decline any query with a structured refusal.

Signatures + Sender Lists + Route Approvals

Every message is authenticated and scoped before it moves through the federation.

Lobster Trap

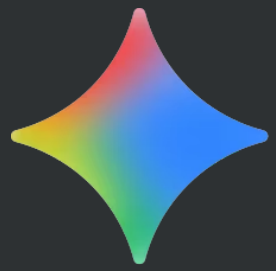
Prompts scanned before model use to block unsafe instructions in real time.

Differential Privacy + Budget Ledger

Noisy aggregates protect individuals; repeated queries are capped by budget.

Hash-Only Identifiers + Audit Trail

Cross-bank matching uses tokens only; all decisions are fully recorded.



Gemini

1 Alert Classification

gemini-2.5-flash

Classifies suspicious local alert candidates after deterministic rules handle obvious cases.

2 Investigation Drafting

gemini-2.5-pro

Drafts narrow 314(b) questions and summarizes peer-bank responses.

3 Graph Finding Explanation

gemini-2.5-flash

Explains graph findings in structuring rings and layering chains

4 SAR Narrative Writing

gemini-2.5-pro

Writes SAR narrative from validated evidence; code computes all required fields.

How Veea's Lobster Trap Works

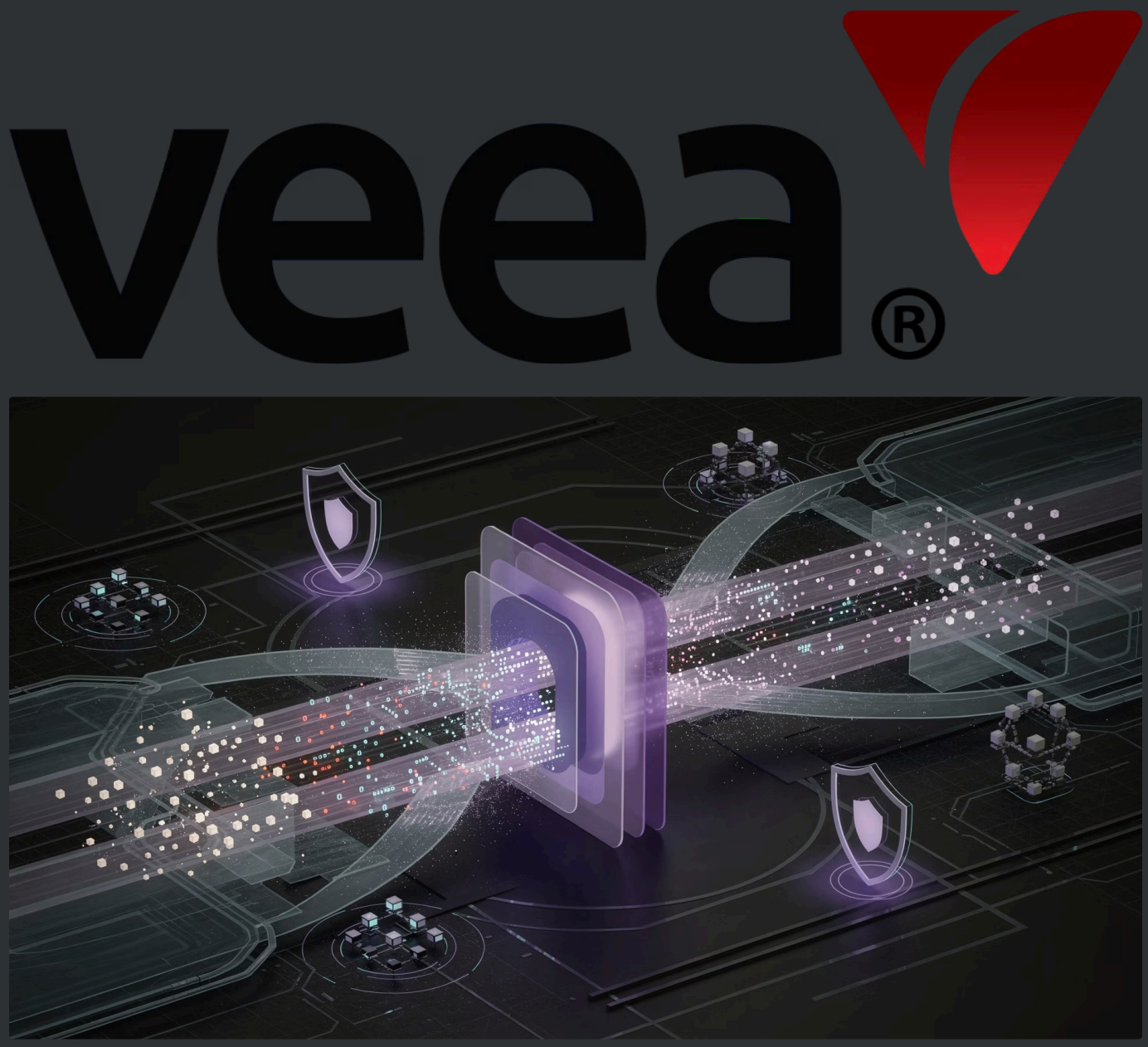
A deterministic LLM security proxy sitting between our agents and Gemini:

> **Agent → Lobster Trap → LiteLLM → Gemini**

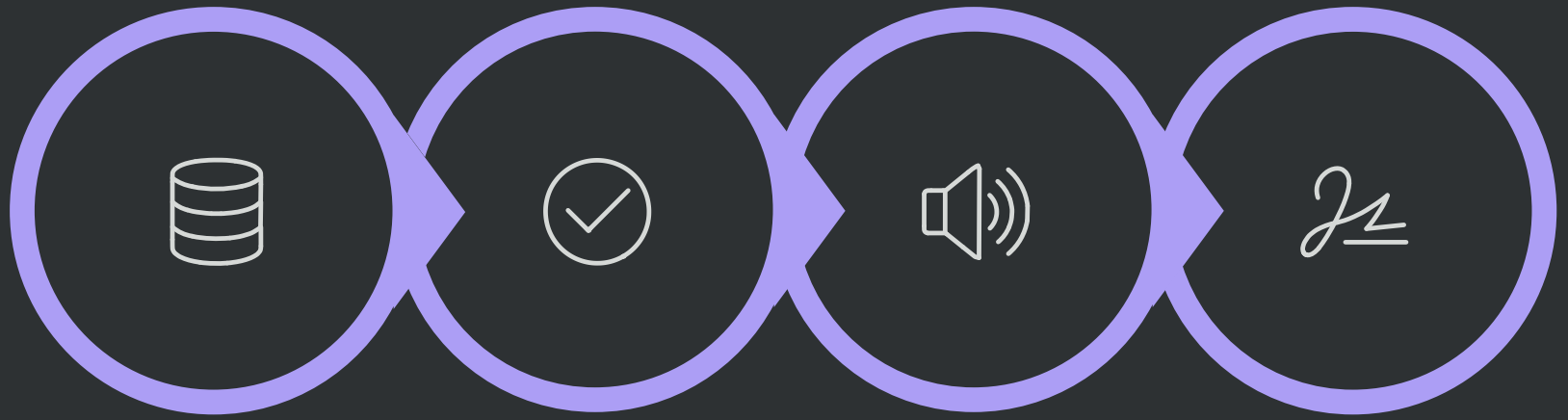
Extracts signals via regex and keyword rules, scores risk with fixed weights, and applies priority-ordered YAML policy. Returns **ALLOW**, **DENY**, **LOG**, or **HUMAN_REVIEW**, with audit metadata showing exactly which rule fired.

Rules Cover

- Prompt injection & evidence fabrication
- Private data requests & hash re-identification
- Audit tampering & privacy budget abuse
- Watchlist leakage & report injection



Differential Privacy Implementation



Query askers are given a privacy budget: if they exceed it the data silo will refuse the request so that the asker can not reconstruct private information.

Raw transactions, customer names, and account records are **never** released. Each requester holds a privacy budget; Gaussian noise is calibrated per query; Signed responses are mathematically proven to be protective of identity.

Generated Investigation Notebooks

Each demo case produces an analyst-style notebook and HTML report showing the full evidence chain:

01

AML Question

Investigator frames a narrow 314(b) request.

02

Protected Bank Statistics

Peer banks return noise-calibrated aggregates only.

03

Federation Combination

Graph, sanctions, and SAR findings assembled.

04

Audit-Ready Output

Reviewers trace the full conclusion; without ever seeing raw customer data.

Market Opportunity

$1.6T

Laundered Globally

Every year — the scale of the problem federated AML targets.

$61B

Compliance Cost

Annual AML compliance spend in the U.S. and Canada alone.

$4.2B

Market by 2030

AML software market growing from $1.7B (2024) — federated AML sells into an existing budget.

Competitive

We view this as reducing legal and compliance spend at affected organizations.

Competitive Landscape

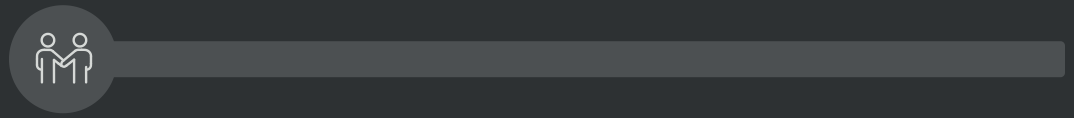
Our solution stands apart by redefining cross-bank collaboration in AML investigations.

1	2	3
Nasdaq Verafin Strong AML network and case platform. Sold to Nasdaq for $2.75B **Why we are different:** Verafin built this for credit unions with contractual privacy; we built it for top-tier banks with technical privacy.	**NICE Actimize** Leading enterprise AML monitoring suite. **Why we are different:** Focuses mostly inside one bank; we focus *between* banks.	**SAS / Oracle FCCM** Mature large-bank compliance infrastructure. **Why we are different:** Also lacks significant cross-bank infrastructure.

Our unique approach focuses on secure, privacy-centric collaboration:

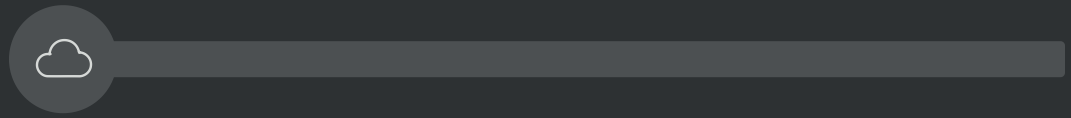
- We focus on cross-bank collaboration, not just single-bank monitoring.
- We let banks share protected statistical intermediaries, not raw records.
- We make Section 314(b) sharing more usable with signed routing, refusals, audit trails, and privacy budgets.
- Lobster Trap and Gemini add a LLM layer that allows for more bespoke data requests while still remaining secure.

What Comes Next



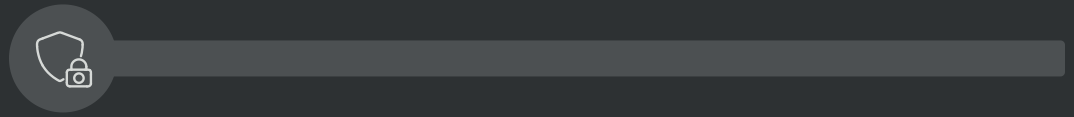
Pilot with Banks

Test with real compliance teams and approved data to validate the federated workflow end-to-end.



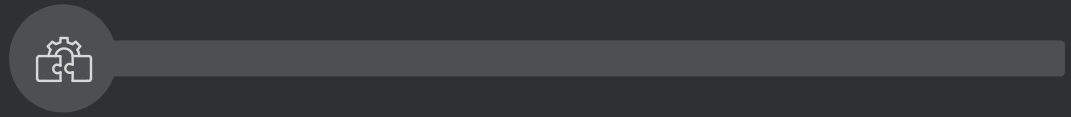
Find early stage partners

Looking for design-partner intros at regional banks that are active §314(b) participants.



Harden Security

Add production key management, real-time monitoring, and a formal incident response plan.



Expand and Integrate

Bank-specific Lobster Trap rules, connections to existing case-management and SAR workflows, and a regulator audit view.