Roe AI for AcquirePay: A Complete Proposal

A Unified Proposal for Proactive Merchant Risk Monitoring – Business Case, Discovery Plan, and Technical Specification

Jaden Fix, Solutions Engineer Candidate, Roe AI

June 30, 2025

Memorandum

To:	AcquirePay Risk Management & Leadership Teams
From:	Jaden Fix, Solutions Engineer Candidate, Roe AI
Date:	June 30, 2025
Subject:	A Unified Proposal for Proactive Merchant Risk Monitoring – Business Case, Discovery Plan, and Technical Specification

Contents

I Solution Brief **3**

1 The Challenge: Evolving and Hidden Risks in the Merchant Portfolio **3**

2 The Solution: Roe AI Lite for Proactive, Continuous Monitoring **3**

3 ROI, Objections, and KPIs: A Clear Path to Value **4**
3.1 Return on Investment (ROI) Metrics 4
3.2 Potential Objections & Counterarguments 5
3.3 Key Performance Indicators (KPIs) 5

II Gap Analysis Guide **6**

4 Introduction: From Vision to Implementation **6**

5 Critical Information Gaps **7**

6 Impact Prioritization and Discovery Questions **8**

7 Anticipating Red Flags (Risks) During Discovery **9**

III Technical Deep Dive **10**

8 Introduction: From Concept to Execution **10**

9 SQL + AI Agent Examples: The Analyst's Experience **10**
9.1 Example 1: Prohibited-Item Keyword Scan 10
9.2 Example 2: AI-Powered Business-Model Classification 11
9.3 Example 3: Multi-Source Reputation & Fraud-Risk Analysis 12

10 Integration Architecture and Performance Considerations **13**

Part I

Solution Brief

1 The Challenge: Evolving and Hidden Risks in the Merchant Portfolio

AcquirePay, a rapidly growing payment processor, faces a persistent challenge: managing hidden risks in a dynamic merchant portfolio. In e-commerce, a merchant's business model and risk profile can shift overnight. They may begin offering products that violate your acceptable use policy, operate in prohibited jurisdictions, or use deceptive marketing; turning a low-risk account into a high-risk one without immediate detection.

This challenge is worsened by the manual, reactive nature of traditional monitoring. Risk analysts often spend hours reviewing merchant websites, social media, and other online sources. The process is labor-intensive, infrequent, and prone to human error; leaving AcquirePay exposed to serious risks:

- **Financial Penalties:** Undetected non-compliant merchant activity can trigger substantial fines from card networks and regulators, often six figures per violation. Regulators have imposed multi-million dollar penalties on processors that ignore illicit conduct [5, 6].
- **Increased Transaction Fraud:** When merchants pivot to high-risk products or shady practices, fraudulent transactions spike. This drives up chargebacks, dispute fees, and fraud rate exposure, resulting in direct losses and higher operational costs.
- **Reputational Damage:** Processing payments for unethical or illegal merchants can harm AcquirePay's standing with banks, card networks, and customers. Trust is difficult to rebuild, and bad press can stall growth. (The FTC recently banned a processor and issued a $5M fine for enabling scams [6].)
- **Operational Inefficiency:** Manual reviews don't scale. High merchant volumes stretch analysts thin, increasing burnout and missed risks. A reactive approach means time is spent on damage control instead of prevention.

At the heart of this challenge is the difficulty of continuously monitoring the vast, unstructured data that reflects a merchant's true activities. Websites change, new products appear, and marketing language evolves, often scattered across the open web. Without automation to interpret this data, risk teams are constantly playing catch-up. Even Roe AI's own research notes that rule-based systems often "fall short of answering these tough questions" about online behavior [4]. In today's landscape, a new approach is needed; one that goes beyond human limits to stay ahead of risky merchants.

2 The Solution: Roe AI Lite for Proactive, Continuous Monitoring

Roe AI Lite is our proposed solution to shift AcquirePay from reactive risk management to proactive, continuous monitoring. It's a specialized configuration of Roe AI's next-gen unstructured data platform [1], purpose-built for merchant risk. Using SQL-based AI agents, Roe AI Lite scans and analyzes merchants' digital footprints in real time; flagging policy violations or risk shifts before they escalate.

Here's how Roe AI Lite directly addresses AcquirePay's key risk challenges:

Table 1: Monitoring Cadence and Latency Paths

Path	Cadence	End-to-End Latency
Nightly Batch Scan	02:00 AM daily	60 minutes
Delta Trigger (event-driven)	On merchant change (webhook / S3 event)	< 5 minutes

- **Automated Web Monitoring:** Roe AI Lite scans each merchant's website HTML and linked policy PDFs for prohibited content (e.g., CBD, gambling terms). Its 24/7 "Prohibited Business Compliance" workflow alerts your team the moment a violation surfaces [2].
- **Analyst-Friendly SQL Rule Engine:** Unlike black-box tools, Roe AI Lite lets analysts define rules using SQL; no coding required. Queries like `WHERE page_text ILIKE '%gambling%'` trigger AI agents to interpret content and flag risks. Analysts can build or adjust checks instantly, using a language they already know [1].
- **Multi-Source Signal Fusion & Alerts:** Beyond websites, Roe AI Lite pulls data from sources like BBB, TrustPilot, and social media [8]. It performs sentiment analysis to detect fraud signals (e.g., "never received product") and pushes real-time alerts into your existing tools (Jira, Slack, etc.)complete with summaries, metadata, and evidence.

Continuous, Scalable Coverage

Roe AI Lite enables true continuous monitoring; scanning thousands of merchants daily and scaling effortlessly with cloud infrastructure. It's not bound by analyst hours or attention span. The moment a merchant updates a website, lists a new product, or goes viral, Roe's AI agents capture and assess the risk. Even the mid-tier plan processes up to 200 web pages per minute [7], ensuring real-time oversight as AcquirePay's portfolio grows.

This isn't just a tool—it's a foundational upgrade to how risk teams operate. Roe AI Lite automates the repetitive, high-volume monitoring that typically consumes analyst hours, allowing your team to focus on complex investigations and decision-making. With 24/7 coverage and evidence-backed alerts, it delivers scalable oversight without analyst fatigue. The outcome is a safer, more transparent merchant portfolio—and fewer costly surprises.

3 ROI, Objections, and KPIs: A Clear Path to Value

3.1 Return on Investment (ROI) Metrics

We understand that any new platform must justify itself in the language of value and ROI. Based on AcquirePay's context, we project Roe AI Lite will deliver tangible returns in several areas:

- **Avoided Fines and Penalties:** Proactive detection of non-compliant merchants will dramatically reduce the incidence of costly fines from card networks and regulators. By catching violations before they escalate, AcquirePay could avoid an estimated 80% of the compliance penalties that might otherwise occur.
- **Analyst Hours Saved:** Automating the routine parts of merchant monitoring will save an enormous amount of manual labor. We estimate at least a 70–80% reduction in time spent on manual website reviews and report writing.
- **Reduced Fraud Losses:** Early identification of high-risk merchant behavior means AcquirePay can act before fraud losses explode. We project a 15–20% reduction in chargeback

and fraud losses associated with merchant misbehavior.

- **Operational Scalability (Cost per Merchant):** With Roe AI Lite, your risk management operations can scale up without a linear increase in cost. You might handle 2–3x the merchants with the same team size, greatly improving productivity.

3.2 Potential Objections & Counterarguments

It's natural for stakeholders to have questions. Below, we address a few likely objections:

- **Objection:** "Our current manual process is managing fine; we've incurred very few fines so far."
- **Counter:** Your risk team is doing a commendable job. However, past success doesn't guarantee future immunity. The risk landscape evolves rapidly. Roe AI Lite acts as a safety net and force multiplier, ensuring that if anything slips past human eyes, the automated system will catch it. It's about moving from managing risk to mastering it.
- **Objection:** "We're concerned an AI system will be complex to implement and maintain."
- **Counter:** Roe AI Lite is designed for accessibility. The interface is SQL, a technology your team already knows. Roe's own team will provide white-glove support for a smooth implementation. Ongoing maintenance is minimal: rules are adjusted with simple SQL edits, and the cloud-based AI agent workforce scales automatically.
- **Objection:** "Budget is tight, how do we justify the cost?"
- **Counter:** Consider the cost of not having it. The potential fines and losses can far exceed the platform's cost. Moreover, the efficiency gains represent a direct cost saving in operational expenses. We can start with a pilot program to demonstrate quick wins and quantify savings, letting the platform justify itself.

3.3 Key Performance Indicators (KPIs)

To ensure Roe AI Lite delivers on its promises, we will jointly track specific KPIs:

- **Compliance Incidents and Fines:** Target a measurable decrease (e.g., 70% reduction) in undetected compliance violations and associated penalties.
- **Detection Speed:** Drastically reduce the "time to flag" for merchant business changes from weeks to near real-time (e.g., 24-48 hours).
- **Fraud/Chargeback Rates:** Target a reduction in fraud and chargeback ratios attributable to merchant misconduct.
- **Analyst Productivity:** Increase the number of merchants monitored per analyst. Use surveys to confirm analysts are spending more time on high-value investigation vs. rote data collection.
- **Stakeholder Satisfaction:** Gauge improved confidence from leadership via feedback and risk committee reports showing fewer "unknowns."

Part II

Gap Analysis Guide

4 Introduction: From Vision to Implementation

The previous section outlined what Roe AI Lite can deliver. Now, we turn to how: What do we need to know to tailor this solution for AcquirePay's specific workflows, systems, and risk thresholds?

This section provides a structured discovery roadmap—a guide to surfacing missing facts, asking the right questions, and identifying potential red flags. Our goal is to co-design an implementation that fits your operational realities, scales with your portfolio, and delivers measurable impact. Rather than taking a one-size-fits-all approach, we focus on uncovering what's essential to make Roe AI Lite succeed in your environment.

5 Critical Information Gaps

Here are the critical discovery areas we'll need to explore with AcquirePay. These gaps directly shape how Roe AI Lite is scoped, integrated, and positioned for maximum impact in your environment. By closing them, we ensure Roe AI Lite doesn't just plug in—it drives real, measurable change from day one.

Table 2: Key Information Gaps

Information Gap	**Why This Matters for Implementation**
Current Merchant Monitoring Workflow	We need to understand your end-to-end process: how merchants are currently reviewed, which teams are involved, review cadence, and escalation paths. This allows us to identify automation points without disrupting critical workflows.
Existing Technology Stack & Data Sources	Knowing your current tooling (e.g., Salesforce, Airflow, Tableau, case management systems) and data locations lets us plan for seamless integration—whether through API, cloud storage, or direct database access.
Operational Cost of Manual Monitoring	Quantifying analyst workload (time spent per merchant/site), tool spend, and false positive rates gives us a baseline for ROI and allows us to simulate cost savings under different automation scenarios.
Risk Policy & "High-Risk" Definitions	Roe AI Lite is only as effective as the rules it enforces. We need detailed criteria: prohibited product lists, geographic restrictions, marketing red flags, and enforcement thresholds—so our AI agents mirror your internal policy with precision.
Team Structure & Stakeholders	To ensure long-term adoption, we must align with key decision-makers (e.g., compliance, risk ops, engineering, exec sponsors) and understand who owns which parts of the risk lifecycle. This prevents misalignment later in the rollout.

6 Impact Prioritization and Discovery Questions

Below is a prioritized list of discovery areas, paired with targeted questions designed to uncover constraints, opportunities, and integration points. These aren't just checkboxes — they're designed to surface the "unknown unknowns" that often derail AI rollouts if left unaddressed.

Table 3: Discovery Questions by Impact

Information Gap	**Impact**	**Key Discovery Questions**
Current Workflow	High	"Can you walk me through the full lifecycle of merchant monitoring — from initial onboarding through risk review and enforcement? What triggers a review (e.g., onboarding rules, complaints, manual audits)? Who handles escalation, and how are cases tracked?"
Tech Stack	High	"What systems currently store merchant metadata and activity logs (e.g., Salesforce, internal DBs)? What orchestration tools are in place (Airflow, dbt, etc.)? How do you currently connect internal tools to external data sources (APIs, web scraping, vendors)?"
Cost of Monitoring	High	"Roughly how many merchants does your team monitor per month? How many FTEs are dedicated to this task? Do you use external vendors or contractors? Can we estimate analyst time per merchant and false-positive workload?"
Risk Policies	High	"Can we review your most recent Acceptable Use Policy and enforcement logic? Are policies centralized or department-specific? What keyword sets, product types, or site behaviors are considered triggers? How often are policies updated?"
Stakeholders	Medium	"Who owns merchant compliance today—Risk, Compliance, Ops, or a shared model? Who needs to be involved in pilot approval, production deployment, and ongoing oversight? How is success measured: precision, coverage, fines avoided, time saved?"

(Note: "High" impact means the project's success heavily depends on that information; "Medium" means it's important but we could proceed with assumptions if needed. There are no "Low" items listed, because we've focused on what really matters.)

7 Anticipating Red Flags (Risks) During Discovery

Table 4: Potential Red Flags and Mitigation Strategies

Red Flag	**What It Might Mean**	**Our Mitigation Strategy**
Vague or Evasive Answers	Key workflows may be undocumented, fragmented, or dependent on tribal knowledge.	We'll offer to co-map the current process live using structured prompts. This lets us clarify hidden dependencies while building trust and shared ownership of the solution.
"We have it under control" Attitude	Signals low urgency or a belief that current systems are sufficient—common in teams without recent incidents.	We'll acknowledge what's working, then use probing questions and industry benchmarks (e.g., enforcement fines, chargeback thresholds) to spotlight where automation improves resilience.
No Access to Key Decision-Makers	May result in stalled adoption, misaligned goals, or lack of technical approvals.	We'll map stakeholder roles early and request access to decision-makers from risk, ops, and IT. We'll tailor messaging to each persona, including executive briefs tied to risk reduction and ROI.
Focus on Features Over Value	Indicates tactical framing—often a sign of a team that's evaluated too many tools without strategic alignment.	We'll shift focus to outcomes by tying each feature to metrics that matter: analyst hours saved, faster detection, reduction in violations. This reframes the conversation around impact, not functionality.

Part III

Technical Deep Dive

8 Introduction: From Concept to Execution

In this section, we transition from the "what and why" into the "how." We'll outline how Roe AI Lite would function within AcquirePay's environment, showcasing concrete examples of SQL queries and AI agent usage. Our goal is to demonstrate that the solution is not vaporware, it's real and achievable.

Note: In the SQL examples below, we use a placeholder function `roe_ai_agent()` to represent calls to Roe AI's agent framework. This simplifies the logic for clarity. The actual implementation involves asynchronously running agents and retrieving results, which our platform handles behind the scenes [3].

9 SQL + AI Agent Examples: The Analyst's Experience

Let's walk through three examples of how an analyst could use Roe AI Lite.

9.1 Example 1: Prohibited-Item Keyword Scan

Scenario (one-liner for business readers):
"Show me any brand-new merchants who are openly selling banned products like vapes or CBD."

Analyst's SQL Query:

```
-- Find any new merchants whose homepage contains prohibited terms.
SELECT
    m.merchant_id,
    m.homepage_url,
    ai_results.output:is_violative_present::BOOLEAN AS is_violative,
    ai_results.output:found_keywords::ARRAY<String> AS detected_keywords
FROM merchants_onboarding_today AS m,
LATERAL (
    SELECT roe_ai_agent(
        m.homepage_url,
        /* JSON config: instruct AI agent to search for keywords */
        '{
            "task_type": "keyword_extraction",
            "parameters": {
                "search_keywords": ["vape", "e-cigarette", "CBD", "kratom", "crypto casino"],
                "case_sensitive": false
            }
        }'
    ) AS ai_results
) AS agent_run
WHERE ai_results.output:is_violative_present = TRUE;
```

Listing 1: Find new merchants with prohibited keywords.

Example JSON Output (for one merchant):

```
{
  "input_url": "http://www.coolvapebro.com",
  "status": "SUCCESS",
  "output": {
```

```
    "is_violative_present": true,
    "found_keywords": ["vape", "e-cigarette"],
    "keyword_context": [
      { "keyword": "vape", "snippet": "...get the best vape juice and mods..." },
      { "keyword": "e-cigarette", "snippet": "...our premium e-cigarette starter kits..." }
    ]
  }
}
```

Plain-Language What-It-Means

- Roe AI skimmed the homepage just like a human analyst would.
- It flagged any banned terms ("vape", "e-cigarette") and captured where they appeared.
- The analyst sees a simple TRUE/FALSE flag plus the exact words—no JSON deep-diving required.

9.2 Example 2: AI-Powered Business-Model Classification

Scenario (one-liner):
"Tell me which merchants have quietly pivoted into selling unregulated health products."

Analyst's SQL Query:

```
-- Classify business type of merchants, and find those offering unregulated consumables.
SELECT
    m.merchant_id,
    m.homepage_url,
    ai_results.output:primary_category::STRING AS business_category,
    ai_results.output:confidence_score::FLOAT AS confidence,
    ai_results.output:supporting_evidence::STRING AS evidence
FROM merchants_under_review AS m,
LATERAL (
    SELECT roe_ai_agent(
        m.homepage_url,
        /* JSON config: instruct agent to classify the business */
        '{
            "task_type": "business_classification",
            "parameters": {
                "classification_categories": [
                    "Standard E-commerce", "Digital Services",
                    "Unregulated Consumables", "High-Risk Financial Services",
                    "Gambling", "Regulated Products"
                ]
            }
        }'
    ) AS ai_results
) AS agent_run
WHERE ai_results.output:primary_category = 'Unregulated Consumables';
```

Listing 2: Classify business types and find those selling unregulated consumables.

Example JSON Output:

```
{
  "input_url": "http://www.zenfulfocus.com",
  "status": "SUCCESS",
  "output": {
    "primary_category": "Unregulated Consumables",
    "confidence_score": 0.92,
    "supporting_evidence": "Our full-spectrum hemp extract contains 1000mg of pure, lab-tested CBD..."
```

```
  }
}
```

Plain-Language What-It-Means

- Roe AI "reads" the site and assigns it a category, not just looks for keywords.
- In this case, it tagged the merchant as "Unregulated Consumables" with 92
- The evidence snippet shows exactly why—mention of high-strength CBD.
- The analyst immediately knows this merchant moved into a riskier product line.

9.3 Example 3: Multi-Source Reputation & Fraud-Risk Analysis

Scenario (one-liner):
"Combine Trustpilot, BBB, and the merchant's own site—alert me if customers are calling it a scam."

Analyst's SQL Query:

```
-- Aggregate multi-source reputation data for high-value merchants.
SELECT
    m.merchant_id,
    ai_results.output:overall_sentiment_score::FLOAT AS sentiment_score,
    ai_results.output:key_complaint_themes::ARRAY<String> AS complaint_themes,
    ai_results.output:fraud_allegation_snippets::ARRAY<String> AS
   fraud_snippets
FROM high_value_merchants AS m,
LATERAL (
    SELECT roe_ai_agent(
        ARRAY_CONSTRUCT(m.homepage_url, m.trustpilot_url, m.bbb_url),
        /* JSON config: instruct agent to synthesize reputation */
        '{
            "task_type": "reputation_synthesis"
        }'
    ) AS ai_results
) AS agent_run
WHERE ai_results.output:overall_sentiment_score < -0.5
   OR ARRAY_SIZE(ai_results.output:fraud_allegation_snippets) > 0;
```

Listing 3: Aggregate reputation data

Example JSON Output:

```
{
  "input_urls": ["...fastfashonz.com", ".../trustpilot...", ".../bbb..."],
  "status": "SUCCESS",
  "output": {
    "overall_sentiment_score": -0.78,
    "key_complaint_themes": ["Shipping Delays", "Billing Issues", "No Customer
    Service"],
    "fraud_allegation_snippets": [
      "Total scam, they took my money and I never received the item."
    ]
  }
}
```

Plain-Language What-It-Means

- Roe AI gathers reviews and profiles from multiple sites and computes an overall sentiment score.
- It lists top complaint themes (e.g., "Shipping Delays") and any direct fraud allegations.
- If the score is very negative (–0.78) or fraud snippets exist, the merchant is flagged automatically.

10 Integration Architecture and Performance Considerations

The diagram below illustrates the updated high-level data flow, including (1) nightly batch coverage of over 20 000 merchants (HTML + policy PDFs), and (2) a real-time change-detection path that publishes a new risk score in under 5 minutes.

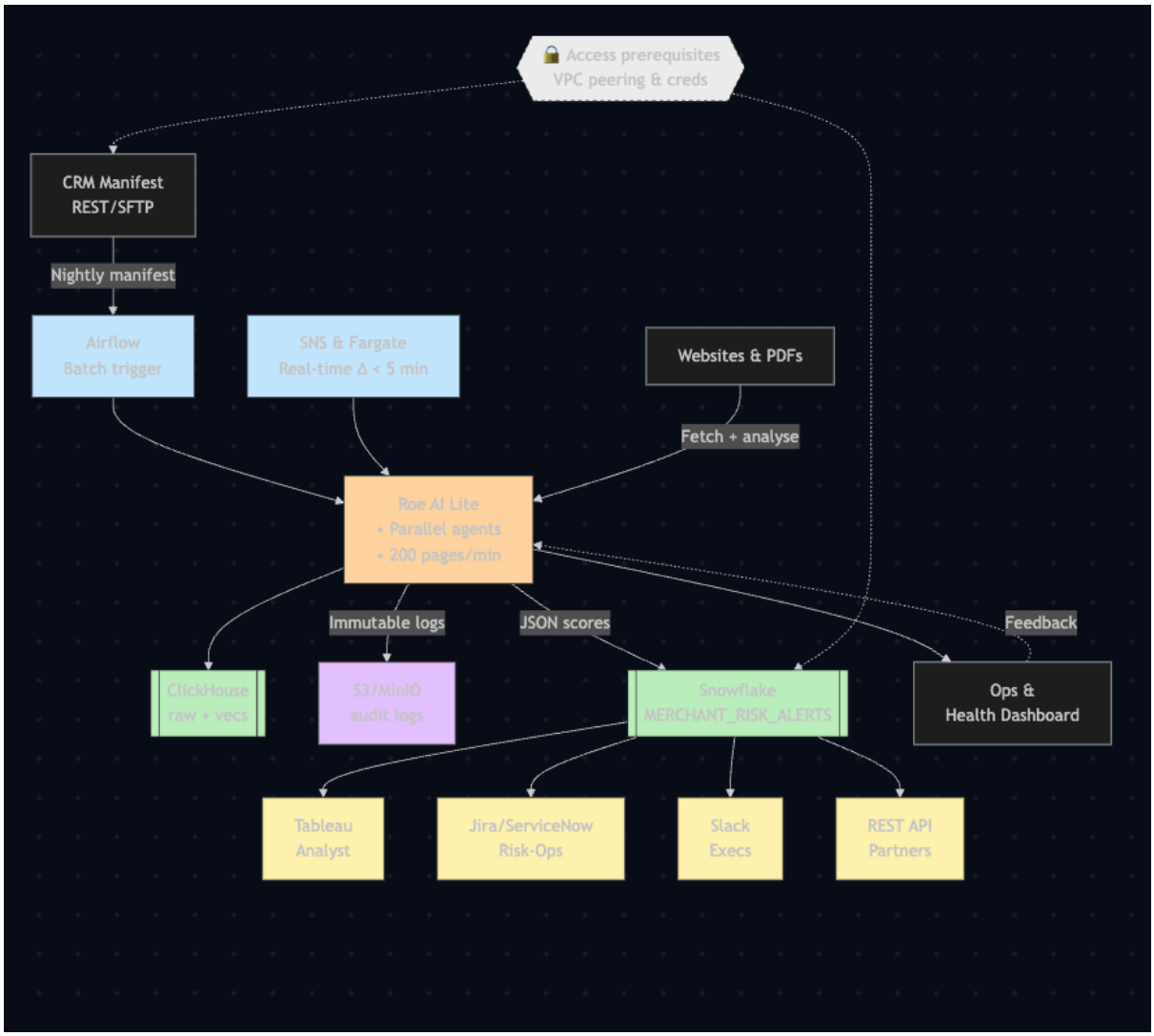

Figure 1: AcquirePay + Roe AI Lite — end-to-end architecture (batch & real-time paths)

1. **Ingestion & Triggers**
   - **Merchant Manifest (CRM).** Read-only REST/SFTP export of ∼20 000 merchants (ID, homepage URL, policy PDF, Trustpilot, BBB).
   - **Batch Path.** Apache Airflow DAG at 02:00 AM invokes `roe_ai_agent(...)`; SLA $<$ 60 min with 200 pp/min $\times$ 4 workers 50 min.
   - **Real-Time Path.** S3 upload $\rightarrow$ SNS $\rightarrow$ AWS Fargate task $\rightarrow$ Roe agent; median end-to-Snowflake latency 3 min, max $<$ 5 min.
2. **Roe AI Lite — Analysis Engine (Core)**
   - **Containerized Workers.** Stateless ECS/Fargate tasks inside Roe's VPC fetch HTML, PDFs & images, then run NLP/CV pipelines (keyword scan, classification, synthesis).
   - **Parallelism & Throughput.** Each worker handles up to 200 pages/minute; auto-scales horizontally for linear performance.
   - **Vector Store & Metadata.** Raw text + vector embeddings stream into ClickHouse; only structured JSON risk rows go downstream.

- **Health Metrics & Feedback.** Queue depth, p99 latency, precision/recall metrics feed into the Ops dashboard for continuous MLOps governance.

3. **Results, Action & Evidence**
   (a) **Snowflake Table `MERCHANT_RISK_ALERTS`.** Stores versioned `risk_score`, rule hits, evidence snippets.
   (b) **Analyst Dashboards (Tableau).** Auto-refresh via live Snowflake connector; provides portfolio heat-maps and drill-downs.
   (c) **Case Management (Jira/ServiceNow).** Snowflake → ticket integration opens cases with severity, snippet, and deep link to raw JSON.
   (d) **Instant Alerts (Slack & Email).** Webhook pushes critical (>0.8) scores to exec channels.
   (e) **Audit Trail (S3/MinIO).** Immutable JSON logs (versioned; Glacier Deep Archive after 5 years).
4. **Performance, Cost & Security Highlights**
   - **Batch SLA Math.** 20 000 merchants × 2 pages 40 000 pages; 1×200 pp/min cluster 3.3 h; 4× clusters → 50 min.
   - **Real-Time Latency.** Median analysis = 3 min; end-to-Snowflake < 5 min (P99 < 7 min).
   - **Cost Efficiency.** All storage is S3-API compatible; PoC runs on free-tier MinIO with zero code changes.
   - **Data-Quality Guards.** Hash-based deduplication, retry logic, quarantine queue to prevent false positives from transient errors.
   - **Security Posture.** Fully inside AWS VPCs; Snowflake via PrivateLink; SOC 2 Type II; AES-256 encryption at rest.

   Bottom line: Roe AI Lite performs the heavy lifting—crawling, inference, and evidence extraction—while Airflow/SNS simply orchestrate triggers and downstream systems handle visualization, ticketing, and audit compliance.

References

[1] Roe AI overview – unstructured data via SQL/AI.

[2] Roe AI compliance workflow for prohibited items.

[3] Roe AI data pipeline integration.

[4] Roe AI blog on challenges of manual web monitoring and AI solution.

[5] Card network rules (Mastercard BRAM, Visa IRP) on fines for acquirers up to six figures.

[6] Recent FTC action against a payment processor (Paddle) for aiding fraudulent merchants – $5M fine, quote on holding processors accountable.

[7] Roe AI performance benchmarks – can process ~200 web pages per minute on mid-tier setup.

[8] Roe AI connectors support data from websites, social media, BBB, TrustPilot, etc., enabling holistic merchant profiles.