Digitizing Fraud Data Reporting, Analytics & Feedback Loop

1 Background & Context

A leading fintech company processes high volumes of UPI and card transactions, accompanied by frequent fraud complaints (stolen cards, unauthorized transactions, phishing). The fraud investigation workflow was completely manual and scattered across Freshdesk, Ops Panel, Google Sheets, emails, and PDF SOPs, causing significant delays and operational risk.

The Crisis: Four Business-Critical Risks

- **a. Delayed fraud response (20–25 mins per case):** Slow blocking led to repeat frauds and increased financial losses.
- **b. Rising fraud losses:** Fraudsters exploited compromised accounts multiple times before they were blocked.
- **c. Regulatory exposure:** Weak fraud controls risked scrutiny from RBI, partner banks, or LEAs — potentially impacting business continuity.
- **d. Customer trust erosion:** Poor fraud handling hurts brand reputation in a competitive payments market.

Why Does This Matter?

This was not an ops problem alone — it impacted:

- **Business continuity:** Regulatory action risk
- **Customer protection:** Faster blocking = fewer victims
- **Competitive positioning:** Market leaders automated; we lagged
- **Scalability:** Manual processes would collapse with transaction growth

Goal: Build a scalable, compliant, data-driven fraud operations capability.

2 Key Stakeholders

Risk Ops Fraud investigation & blocking	**Product (Fraud & Payments)** Rule optimization, analytics	**Compliance** RBI/NPCI reporting	**Engineering** Ops panel & backend services	**Customer Support** Ticket routing via Freshdesk

3 Manual Process (Before Digitization)

Step	Time	Description
1. Ticket Assessment	3 min	Extract details manually from Freshdesk
2. Data Gathering	4 min	Check 4 Ops modules for data
3. Proof Compilation	5 min	Manual creation of Doc to be uploaded on Freshdesk
4. Blocking Actions	6 min	Manual blocking of the involved systems
5. Phishing Sheet	3 min	Data entry into the google sheets posing risk of exposure
6. Ticket Closure	2 min	Manual updates in Freshdesk
Total Time:		**~23 minutes per ticket**

Scale impact example: 5,000–6,000 cases/month → 1,900–2,300 ops hours/month (not counting Product/Compliance rework)

4 Pain Points Identified

Data Fragmentation: Data across 5+ systems, no single transaction/user view, manual proof collation

Inconsistent Blocking & Errors: Ambiguous manual SOP, missing linked entities (IMEI, IP, VPA, device), No automated mapping logic

Phishing Sheet Vulnerabilities: Manual, error-prone, no validation, not scalable and sensitive data in shared sheets

Delayed Feedback Loop: No fraud trend analysis, slow risk rule optimization, manual fraud-spike detection

High Turnaround Time: High manual work leading to not detailed investigations

5 Solution Overview

To transform the manual fraud workflow into a scalable, data-driven system, I designed an end-to-end digitized solution that unified data, automated repetitive actions, streamlined blocking, and enabled real-time reporting.

• Single-Screen Fraud Investigation Workspace

- **Transaction Locator:** Enter LEA details to locate exact transactions
- **Stolen Card Data Entry:** Record fraud information systematically
- **Search Interface:** Historic fraud search with filters and timeframes
- **Backend System:** Coordinates systems to flag transactions and block credentials

• System-Driven Blocking Engine

"Smart Blocking" engine auto-suggested actions based on case type. Mapped blocking rules: User ID, Wallet, Bank account, UPI ID/VPA, Device/IMEI, IP address.

Blocking time: 6 mins → ~1 min with fewer misses

• Integrated Fraud Data Store & Phishing Repository

Created dedicated fraud database, structured schema, replaced phishing sheet with internal module, automatic ingestion, audit logs & validations.

Zero dependency on external sheets

• Fraud Analytics Dashboard & Feedback Loop

Real-time dashboard: Fraud type frequency, repeat offender detection, source vector trends, rule performance, alerting system, monthly insights to Risk Product.

Faster rule tuning + reduced recurring fraud

6 Overall Impact of Digitization

70% Processing Time Reduction (23 → 7 mins per case)	**47%** Repeated Fraud Loss Reduction	**90%** Reduction in Escalations
2x Team Capacity Without Headcount Increase	**1,300+** Ops Hours Saved Monthly	**100%** Scalable for New Product Launches

Operational Efficiency: Enabled team to handle 5,000-6,000 cases/month with same 10-agent capacity (previously would have required 18-20 agents)

Fraud Prevention: Faster blocking and entity-link detection enabled identification of new fraud patterns & trends quickly, reducing repeat fraud by 47%

Regulatory Compliance: Achieved 90% reduction in escalations with complete audit trail, standardized reporting, and reduced RBI/bank escalation risk

Strategic Value: Product teams received structured fraud insights enabling faster rule optimization; system scalable for newly launched products without additional overhead

7 My Role in This Transformation

- ✓ Led end-to-end discovery of manual process, pain points, and bottlenecks
- ✓ Created requirement docs, workflow designs, and blocking automation logic
- ✓ Partnered with Ops, Product, Engineering, and Compliance to finalize future-state workflow
- ✓ Designed data schema for fraud repository
- ✓ Worked with engineers to validate system behavior and edge cases
- ✓ Drove rollout, testing, and change management across Risk Ops
- ✓ Set up dashboards and feedback loops for ongoing monitoring and rule optimization

View Prototype →