Digitizing Fraud Data Reporting, Analytics & Feedback Loop

1. Background & Context

Freecharge 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)

The goal was to 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

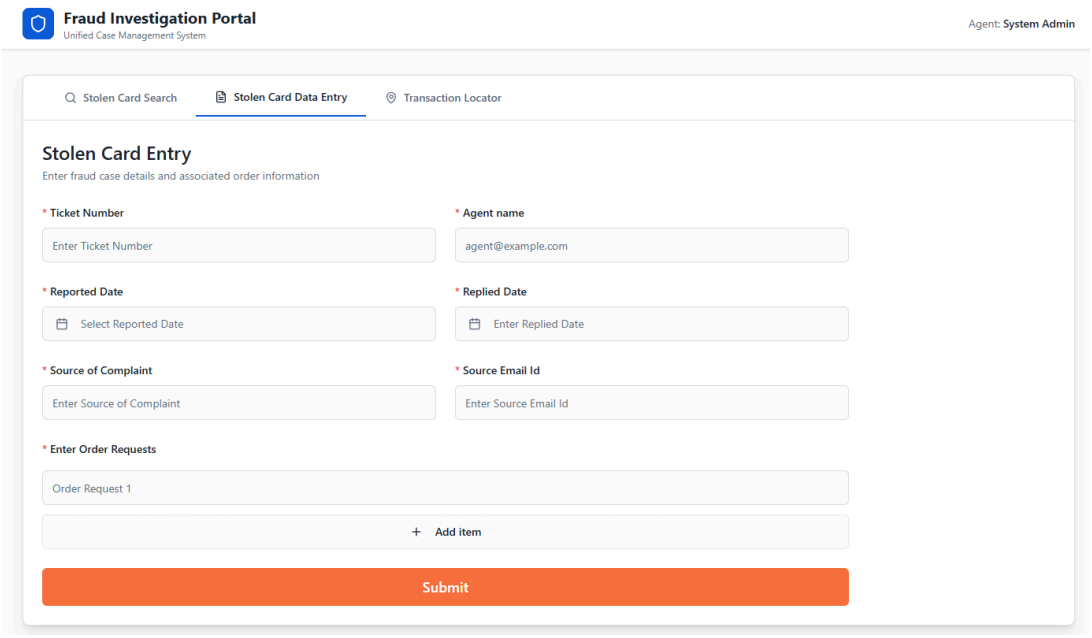
Category	Key Issues
Data Fragmentation	Data across 5+ systems, no single transaction/user view, manual proof collation
Inconsistent Blocking & Errors	Ambiguous manual SOP, missing linked entities (IMEI, IP, VPA, device), No automated mapping logic
Phishing Sheet Vulnerabilities	Manual, error-prone, no 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

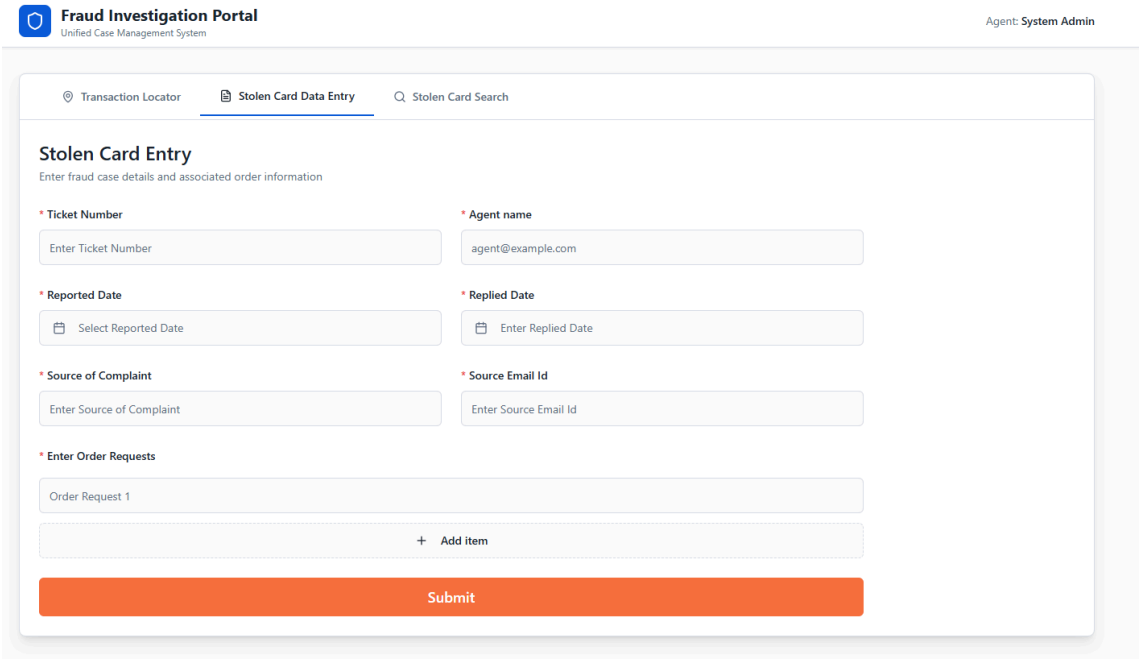
5. Solution Overview

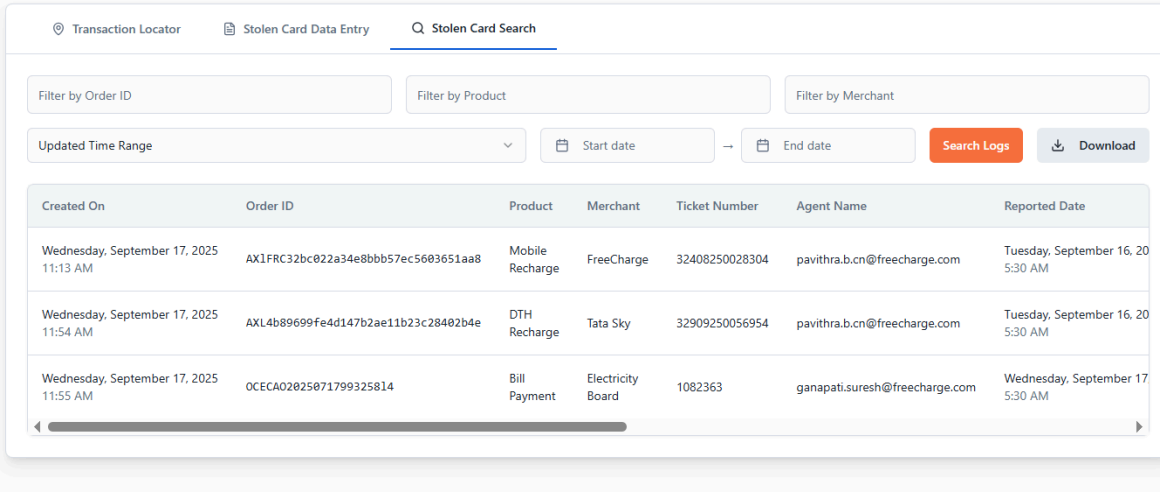
To transform the manual fraud workflow into a scalable, data-driven system, I designed an end-to-end digitized solution that unified data, automated repetitive actions, streamlined blocking, and enabled real-time reporting. The goal was to shift the process from people-dependent to system-driven, while ensuring compliance, operational accuracy, and faster fraud mitigation.

- Single-Screen Fraud Investigation Workspace -
    - Transaction Locator - A tool that interacts that allows the executive to enter necessary details provided by the LEA to locate the exact transactions.

- Stolen Card Data Entry - An interface that allows the system to record the exact information related to fraud raised.
- Search - An interface that allows the users to search the historic reported frauds based on certain filters and input of time frame.
- Backend system - That enables to coordinate with various systems to flag the fraudulent transactions, get the details, block the necessary user details like user id, vpa, cards etc.







- System-Driven Blocking Engine - “Smart Blocking” engine auto-suggested or preselected actions based on case type. Reduced human error by enforcing SOP logic in the system
    - Mapped blocking rules for all linked entities:
        - User ID, Wallet, Bank account, UPI ID / VPA, Device/IMEI, IP address

Outcome: Blocking time reduced from 6 mins → ~1 min with significantly fewer misses.

- Integrated Fraud Data Store & Phishing Repository
    - Created a dedicated fraud database table
    - Structured schema for reports, fraud metadata, and blocking info
    - Replaced phishing sheet with an internal module
    - Automatic ingestion from Freshdesk + Ops Panel
    - Audit logs, validations, and permission controls

Outcome: Zero dependency on external sheets; scalable and secure.

- Fraud Analytics Dashboard & Feedback Loop to Product - Real-time dashboard covering:
    - Fraud type frequency
    - Repeat offender detection
    - Source vector trends (device/IP clusters)
    - Rule performance & false positives
    - Alerting system for fraud spikes
    - Monthly insights shared with Risk Product for rule updates

Outcome: Faster rule tuning + measurable reduction in recurring fraud patterns.

6. Overall Impact of Digitization

- Operational Efficiency

    - Total handling time reduced:
      23 mins → 7 mins per case (70% reduction)
    - 5,000–6,000 cases/month → 1,300+ hours saved monthly

- Fraud Loss Reduction
    - Faster blocking reduced repeat exploitation of compromised accounts
    - Stronger entity-link detection enabled proactive prevention

- Regulatory Strengthening
    - Ensured traceability, auditability, and standardized fraud reporting
    - Reduced risk of RBI/bank escalations due to poor controls

- Improved Cross-Team Collaboration
    - Product teams now received structured fraud insights
    - Risk & Compliance teams had reliable data stores and dashboards
- Scalability
    - System built to handle multi-fold transaction growth without needing more manpower

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 the future-state workflow
- Designed the 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

Prototype of Digital tool - https://vigil-workspace.lovable.app/