EARLY DETECTION OF SYNTHETIC ACTORS ON DIGITAL PAYMENT PLATFORMS

Fraud Detection System – Use Case 1

Team: Chip & Clip

Team Members
A.Keerthana
Sanjay.G
Siddharth.V

PROBLEM OVERVIEW

- Synthetic identities blend real and fake attributes to bypass onboarding checks
- Early behavior appears normal, delaying detection
- Fraud risk emerges only after cross-signal correlation
- Late detection leads to financial loss and customer friction

OBJECTIVE

Detect synthetic actors **before material loss** while preserving customer experience

SUCCESS CRITERIA:

- EARLY-STAGE RISK IDENTIFICATION (PRE-TRANSACTION / EARLY USAGE)
- REDUCED FALSE POSITIVES FOR LEGITIMATE USERS
- EXPLAINABLE, AUDIT-READY DECISIONS
- PROPORTIONAL SECURITY CONTROLS

FRAUD ANALYST PERSONA

Name : ROHAN MEHTA

Demographics

Age: 34

Location: Mumbai / Chennai (Global Delivery Center)

Role: Senior Fraud Operations Analyst

Experience: 9 years in payments & fraud monitoring

"I don't need more alerts. I need the right ones - with reasons I can trust."

Needs & Goals

Catch fraud early, before losses escalate

Clear risk explanations, not black-box scores

Ability to prioritize alerts that actually matter

Fast decision-making under pressure

Challenges

Alert fatigue from false positives

Fragmented signals across devices, behavior, and transactions

Pressure to balance customer experience with security

Limited time per case during fraud spikes

COMPLIANCE OFFICER PERSONA

Name : Anurag Arora

Demographics

Age: 45

Location: New York

Role: Senior Compliance & AML Officer

Experience: 18+ years in financial regulation

Needs & Goals

- Regulatory adherence (KYC, AML, SARs)
- Explainable decisions for auditors and regulators
- Consistent policy enforcement across regions
- Confidence that controls will hold up under scrutiny

Challenges

- Interpreting evolving regulations
- Aligning fast AI systems with slow regulatory frameworks
- Ensuring fairness and non-discrimination
- Managing risk without stalling innovation

“If we can’t explain it to a regulator, we can’t deploy it.”

DATA SCIENTIST PERSONA

Name : Meera Iyer

Demographics

Age: 29

Location: Bangalore

Role: Senior Data Scientist, Fraud & Risk.

Background : AI/ML, Graph Analytics

Experience: 9+ years in financial regulation

"Fraud doesn't repeat itself - it mutates. Our models must adapt faster."

Needs & Goals

- High-quality, well-labeled data
- Ability to test models without impacting live customers
- Early detection of new fraud patterns (not yesterday's fraud)
- Reduced bias and explainability in models

Challenges

- Synthetic identities evolve faster than models
- Ground truth is delayed or incomplete
- Pressure to reduce false positives without lowering recall
- Translating model outputs into business language

THE FRAUDSTER PERSONA

Name : Shadow Weaver

Demographics

Age: Unknown

Location: Distributed/Cross-Border

Role: Organized fraud operator specializing in synthetic identities

“Fraud isn’t about stealing fast - it’s about waiting patiently.”

Needs & Goals

- Build identities that pass early checks
- Blend into legitimate customer populations
- Scale fraud without triggering alerts
- Evade device, behavioral, and KYC linkages

Challenges

- Identity graphs eventually expose weak links
- Reuse of infrastructure creates detectable clusters
- Behavioral drift over time
- AI-based anomaly detection improves continuously

THE LEGITIMATE CUSTOMER PERSONA

Name : Saira Khan

Demographics

Age: 32

Location: Delhi NCR

Profession : Product manager at a mid-sized tech firm

Daily Behaviour : Daily digital payments, UPI + cards + international transactions

“Protect my money - but don’t make me feel like a criminal.”

Needs & Goals

- Fast, uninterrupted payments
- Confidence that her money is protected
- Clear communication when security checks occur
- Control over her own account security

Challenges

- Occasional MFA prompts during travel
- Account flags triggered by unusual but legitimate behavior
- Anxiety when transactions are delayed without explanation
- Fear of losing access during critical moments

Journy Map

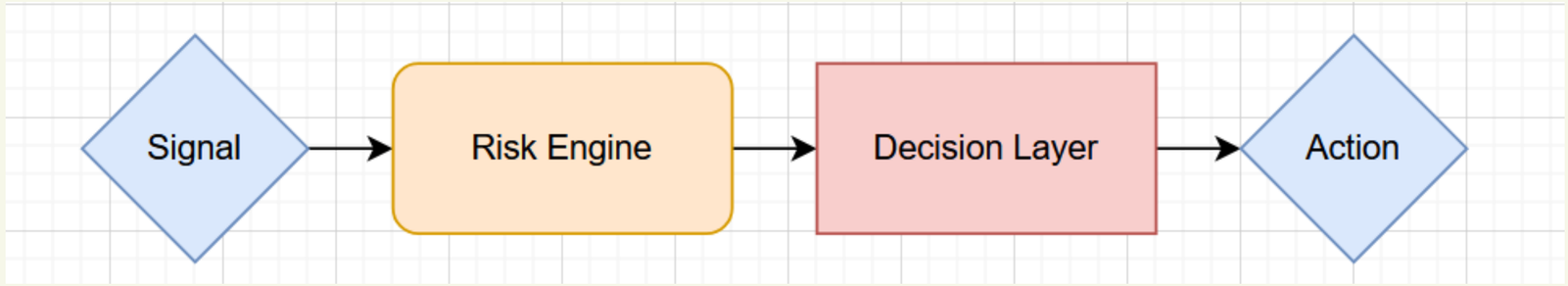
	Onboarding	Early Usage	Risk Assessment	Intervention	Feedback Loop
User Actions (Activities)	Signs up • Submits KYC	• Adds funds • First transactions	• No visible action	• Receives MFA / hold	• Account resumes / blocked
Touchpoints (Interaction Points)	• Signup screen • KYC upload	• Wallet / UPI interface	• Fraud analyst dashboard	• OTP / notification • Support message	• Analyst tools • Audit logs
System Intelligence (Thought Bubbles)	• Device fingerprinting • Identity consistency checks	• Behavioural analysis • Velocity monitoring	• Risk score aggregation • Identity graph expansion	• Confidence-based decisioning	• Analyst labels • Model updates
Pain Points / Risk Signals	• Synthetic ID appears legitimate	• Low-value but repetitive transactions	• Hidden account linkages	• Risk of false positives	• Delayed learning without feedback
Opportunities / Interventions	• Early-stage risk score	• Cross-signal correlation	• Explainable risk insights • Graph-based clustering	• Progressive friction (MFA / hold)	• Continuous risk refinement

PROGRESSIVE RISK CONFIDENCE INCREASES →

JOURNEY INSIGHTS

- Synthetic actors appear legitimate during onboarding
- Device and behavioral signals surface risk earlier than transactions
- Identity graphs expose coordinated activity
- Progressive friction reduces customer impact

SOLUTION ARCHITECTURE



- Signal federation across identity, device, and payments
- Identity graph for relationship analysis
- Risk-based, explainable decisions

DESIGN PRINCIPLES

1. **Signal Federation**

Login, device, KYC, transaction data unified

2. Identity Graph Intelligence

Detect shared infrastructure and clusters

3. Progressive Friction
Silent checks → MFA → hold/review

MINIMUM VIABLE PRODUCT (MVP)

Included in MVP

Risk scoring engine (rules + ML)

Fraud analyst dashboard

Identity graph visualization

Risk-based escalation logic

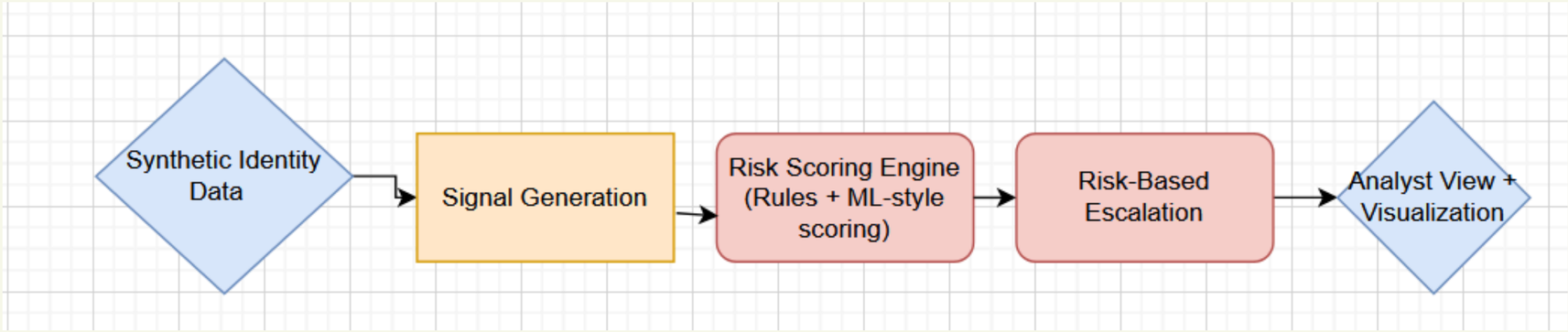
Out of Scope

Live payment rails

Production KYC integrations

Full-scale ML retraining

PROTOTYPE OVERVIEW



WHY THIS FLOW IS EFFICIENT

No real data dependency
No heavy ML infrastructure
Early detection before loss
Clear upgrade path (graphs, federated learning later)

PROJECT OVERVIEW

Synthetic Identity Fraud – Analyst Dashboard

Early Detection | Risk-Based Escalation | Minimalist MVP

Risk Scoring Engine

Signals Used

- Login Velocity
- Transaction Amount Spike
- Device Reuse Score
- Session Regularity
- Account Age Mismatch

Escalation Logic

Risk Score	Action
< 0.30	Allow
0.30 – 0.60	Silent Check
0.60 – 0.80	MFA Trigger
> 0.80	Hold / Review

Fraud Analyst View

Identity Risk Table

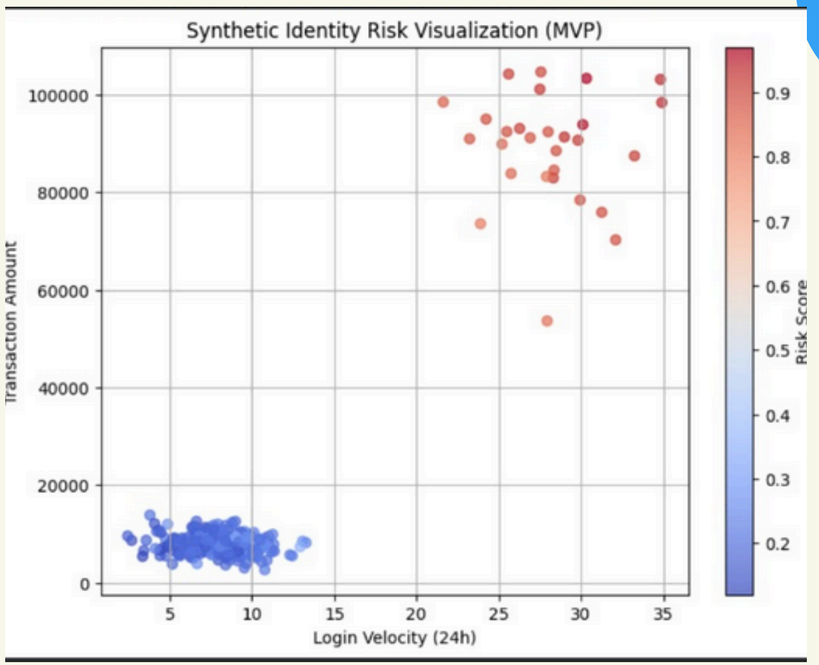
Identity ID	Risk Score	Status
ID_1021	0.18	Allowed
ID_2043	0.57	Silent Check
ID_3307	0.84	Hold

Identity Graph (Conceptual)

ID · Device · Account · Txn

Clustered nodes indicate synthetic identity patterns.

MVP Demo – Synthetic Data Only



JOURNEY-TO-MVP ALIGNMENT

Journey Stage	MVP Capability
Onboarding	Device & identity risk scoring
Early Usage	Behavioral & velocity analysis
Risk Review	Analyst dashboard
Intervention	Progressive friction logic
Feedback	Analyst labeling loop

THANK YOU