End-to-End Financial Fraud Case Study & Solution

A Comprehensive Fruad analysis and advance Fraud detection
System

Contents

Introduction	Problem statement and dataset overview.
Understanding Fraud behaviour	Fraud patterns by account, transaction type, time, and balance behavior.
Solution	LightGBM-based fraud detection approach.
Impact	Fraud detection performance and outcomes.

01

Introduction

Introduction

Financial fraud is a critical challenge in digital payment systems, where fraudulent transactions are rare but cause significant financial loss.

Traditional monitoring systems often apply uniform checks across all transactions, leading to high operational cost and poor fraud detection.

This project focuses on understanding fraud behavior using exploratory data analysis (EDA) and designing a LightGBM-based fraud detection model that prioritizes high risk transactions.

The objective is to maximize fraud detection while minimizing false alerts and manual reviews.

Dataset Overview

The dataset represents 30 days of transaction activity,
where each step equals 1 hour (total 744 hours).

Each record captures a single financial transaction, including:

Transaction type (CASH-IN, CASH-OUT, DEBIT, PAYMENT, TRANSFER)
Transaction amount
Sender and receiver account details
Account balances before and after the transaction

Fraud labels are provided:

isFraud indicates whether a transaction is fraudulent
isFlaggedFraud represents a simple rule-based flag
(transfer amount > 200,000)

Fraud in this dataset mainly involves account takeover,
where money is transferred to another account and then cashed out.

02

Frauds Behaviour

Account Type

- No fraudulent transactions occur when a Merchant (M…) account is involved
- Applies to:
    - Merchant → Customer
    - Customer → Merchant
    - Merchant → Merchant
- All fraud occurs exclusively between Customer ↔ Customer (C…) accounts
- Why This Matters

- Merchant accounts behave as trusted entities
- Fraudsters exploit peer-to-peer customer transactions

Focus fraud detection only on Customer-to-Customer flows.
Merchant transactions can be de-prioritized.

Account Type

❑ Analysis shows that no fraud occurs when a Merchant (M…) account is involved, either as sender or receiver.

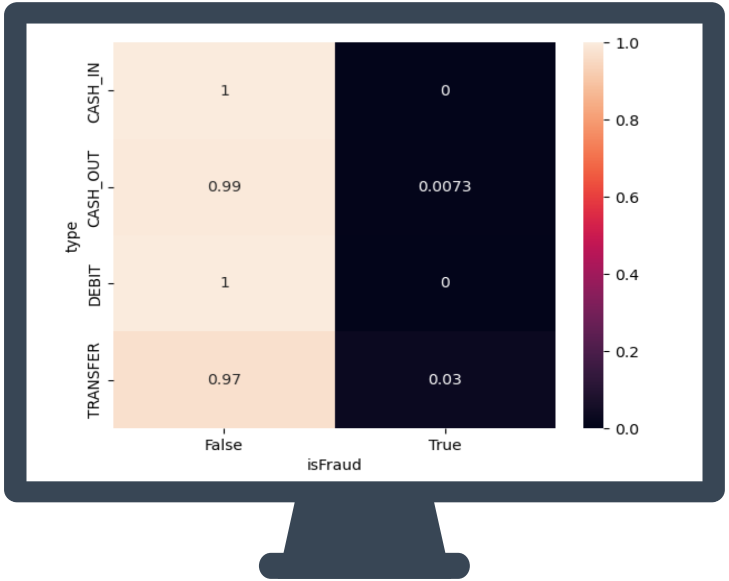
❑ Transactions such as:
Merchant → Customer
Customer → Merchant
Merchant → Merchant have zero fraud cases in the dataset.

❑ All fraudulent transactions are observed only between
Customer ↔ Customer (C…) accounts.

❑ Takeaway:
Fraud detection should focus on Customer-to-Customer transactions, while Merchant-related transactions can be considered low risk.

Transaction Type

- Fraud is observed only in two transaction types:
  - TRANSFER → ~3% fraud (highest risk)
  - CASH_OUT → ~0.7% fraud
- CASH_IN and DEBIT show 0% fraud across the dataset.
- TRANSFER is the most risky transaction type:
  - Highest fraud concentration
  - Matches real-world fraud flow:
    Money is transferred → then cashed out
- CASH_OUT is the second most risky:
  - Used mainly to withdraw stolen money
  - Fraud rate is lower than TRANSFER but still significant
- Key Takeaway:
  Fraud is not random. It is highly concentrated in TRANSFER and CASH_OUT, while CASH_IN and DEBIT are low-risk and require minimal monitoring.



Transaction Time

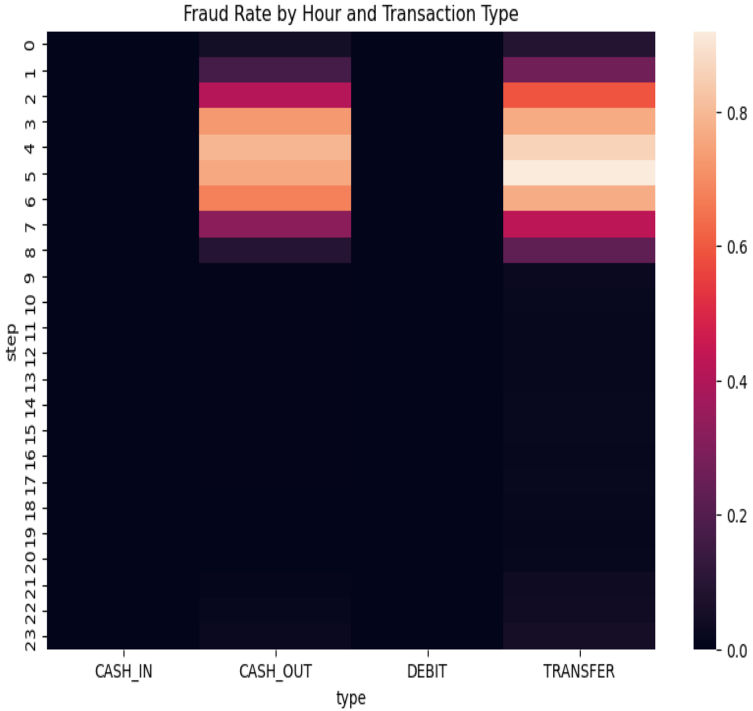
- Fraud is highly concentrated during late-night to early-morning hours (≈ 1 AM – 7 AM).

- During daytime hours, fraud occurrence is almost zero across all transaction types.

- Fraud activity at night is observed mainly in:
  - TRANSFER
  - CASH_OUT

- TRANSFER shows the strongest fraud signal at night, indicating that fraudsters prefer transferring money between accounts during low-monitoring hours.

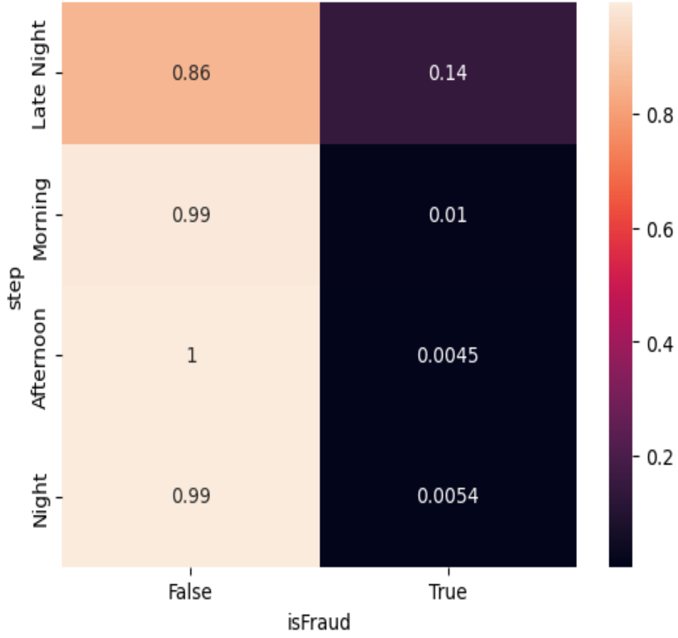
- Key Takeaway:
  Fraudsters exploit late-night hours when monitoring is low and primarily use TRANSFER and CASH_OUT transactions to move money quickly.



Transaction Time

- Late Night transactions show extremely high fraud concentration:
  - Around 14% of late-night transactions are fraudulent
  - This is significantly higher than any other time bucket.
- Morning transactions are mostly safe:
  - Fraud rate is approximately ~1%
  - Indicates dominance of normal user activity.
- Afternoon is the safest period:
  - Fraud rate around ~0.45%
  - Lowest fraud occurrence across the day.
- Evening (Night) shows slightly higher fraud than afternoon:
  - Fraud rate around ~0.54%
  - Still much lower compared to late night.
- Why this pattern exists
- Late night:
  - Reduced monitoring
  - Users inactive or sleeping
  - Fraudsters exploit low vigilance
- Daytime:
  - Normal transactional behavior
  - Higher user awareness
- Key Takeaway:

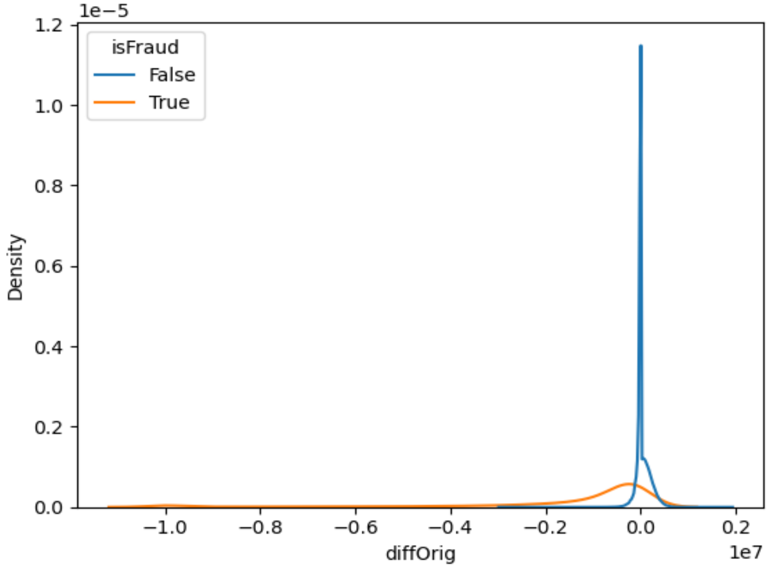
  Late Night is the highest-risk time bucket, while daytime transactions are largely safe and require lighter monitoring.



Sender Balance Change

- Non-fraud transactions are highly concentrated around zero balance change,
  indicating normal transactions with minimal impact on the sender’s account.

- Fraud transactions show much larger balance changes, with a long tail,
  reflecting sudden and abnormal money movement.

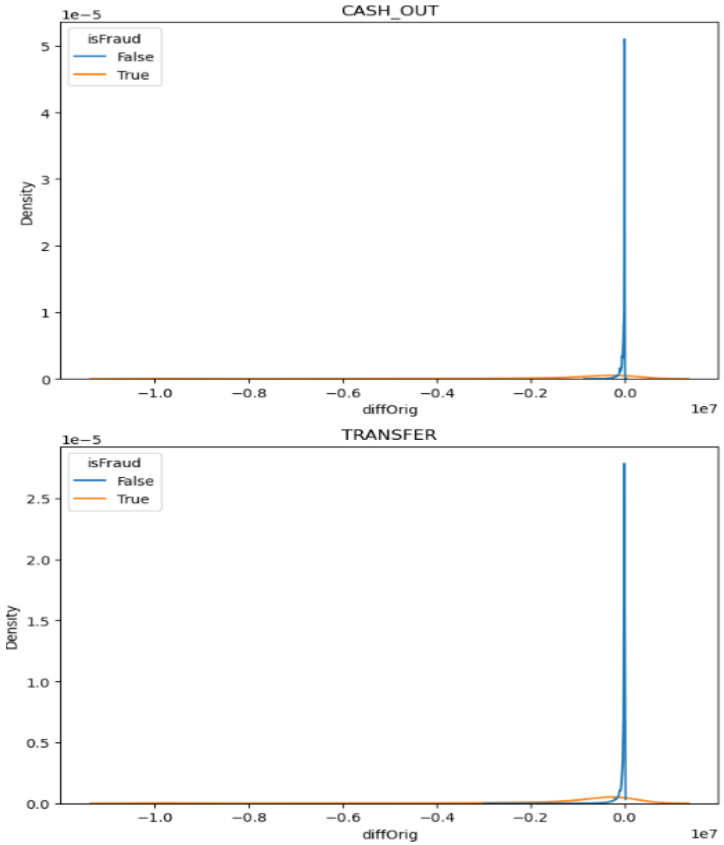


Sender Balance Change

- In CASH_OUT transactions:
  - Fraud cases show large negative balance changes
  - Sender accounts are often fully or heavily drained

- In TRANSFER transactions:
  - Fraud involves larger balance reductions compared to non-fraud
  - Non-fraud transfers usually cause small, controlled changes

- Takeaway:
  Sudden and unusually large reductions in sender balance are a strong indicator of fraud, especially for TRANSFER and CASH_OUT transactions.

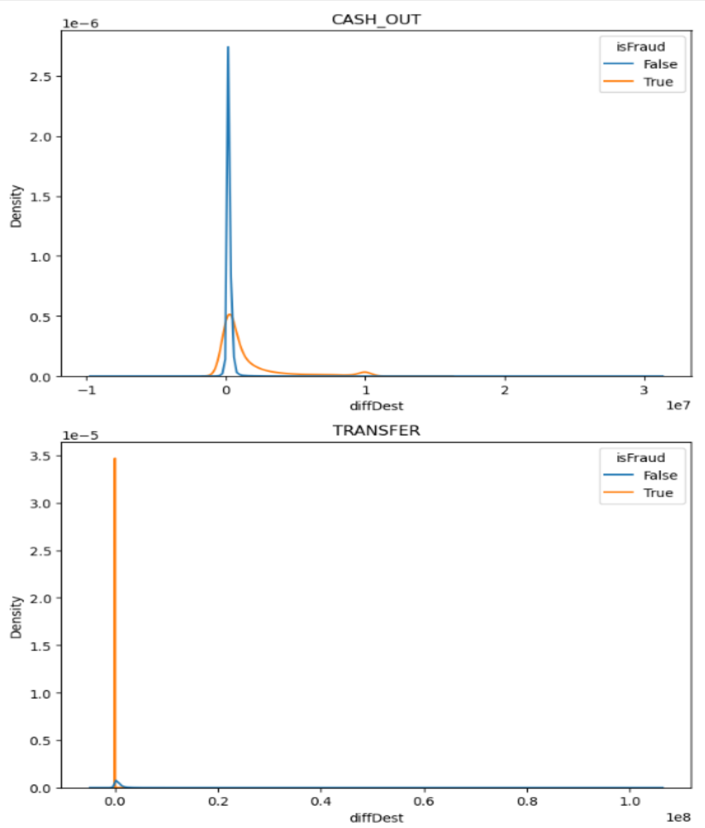


Destination Balance Change

- Fraud activity is mainly observed in TRANSFER and CASH_OUT transactions.

- In CASH_OUT transactions:
  - Receiver balance does not change
  - As a result, diffDest looks similar for both fraud and non-fraud cases
  - Destination balance is not a reliable signal for CASH_OUT fraud
- In TRANSFER transactions:
  - When diffDest = 0, the probability of fraud is very high
  - Normal (non-fraud) transfers usually show a positive destination balance change

- Takeaway:
  For TRANSFER transactions, a zero destination balance change (diffDest = 0) is a strong fraud indicator, while normal diffDest values are mostly associated with non-fraud.

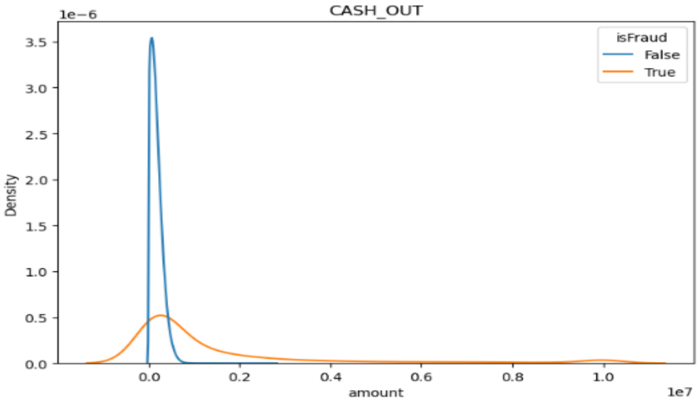


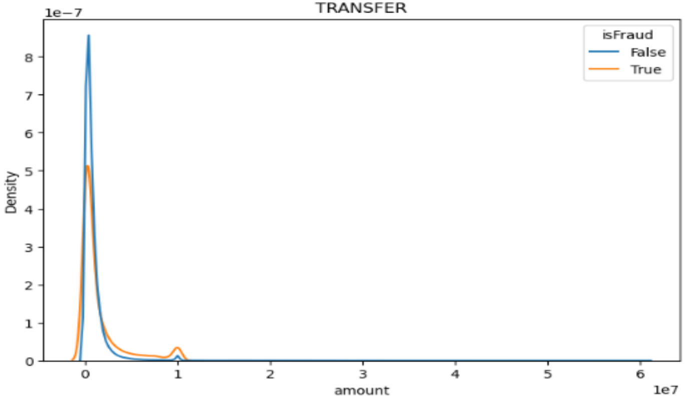
Amount Distribution

- CASH_OUT transactions:
  - Fraud transactions occur at significantly higher amounts
  - Non-fraud transactions are tightly concentrated at lower amounts
  - Indicates high-risk large withdrawals

- TRANSFER transactions:
  - Fraud and non-fraud amounts overlap
  - However, fraud shows a heavier right tail
  - Large transfers are more frequent in fraud cases
  - TRANSFER acts as the primary fraud channel

- Takeaway:
  Fraud is associated with larger transaction amounts, especially in TRANSFER and CASH_OUT, while CASH_IN and DEBIT remain low risk.





03

SOLUTION

Solution Overview

How We Designed the Fraud Detection Solution

- Our EDA clearly showed that fraud is not random
- Fraud is concentrated around specific transaction types, time windows, and
- balance behaviors
- This means a rule-only system is insufficient

What was needed

- A model that can combine multiple fraud signals together
- A system that can adapt to complex, real-world fraud patterns

LightGBM was chosen as the core model to meet these needs.

Primary Objective

- Detect maximum fraud
- While keeping false alerts and manual review low

Why LightGBM?

Why LightGBM Fits This Problem

- Fraud data is highly imbalanced → LightGBM handles this well
- Fraud patterns are non-linear and multi-dimensional
- LightGBM learns interactions between time, amount, and balance changes
- Fast and scalable for real-world deployment
- Provides feature importance, helping with explainability

Why not rules alone?

- Rules are static
- Fraud behavior evolves
- Rules alone miss unseen and subtle fraud patterns
- LightGBM gives flexibility + intelligence, beyond hard rules.

Modeling Strategy

Fraud Detection Strategy

- LightGBM binary classification model
- Optimized for high fraud recall
- Uses probability-based decision thresholds

- **Combines multiple signals together:**
  - Transaction type
  - Time of day
  - Amount Balance changes

Design Philosophy

It is better to catch fraud early and review borderline cases than to let fraud pass silently.

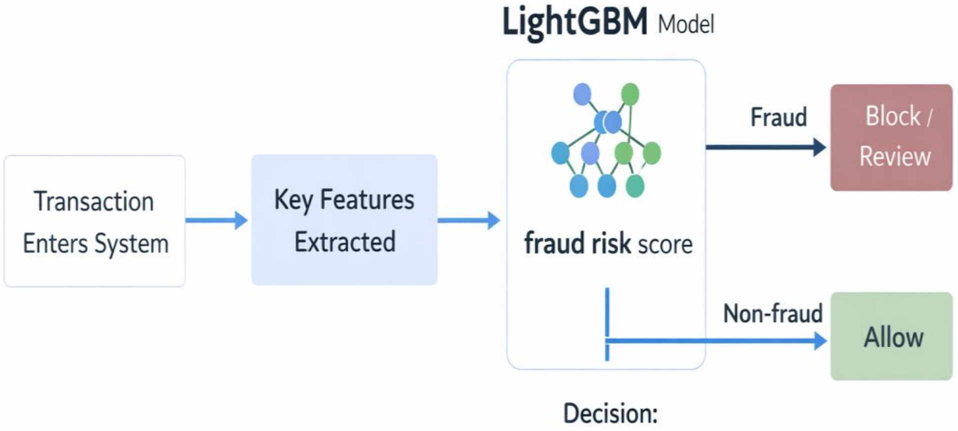
This ensures strong protection without aggressive blocking.

Solution Architecture

How the System Works (High-Level)

- A transaction enters the system
- Relevant risk features are extracted
- LightGBM assigns a **fraud risk score**
- Based on risk:
    - **High risk → Block**
    - **Medium risk → Review**
    - **Low risk → Allow**

The flow is **simple, scalable, and production-ready**



Modeling Strategy

Fraud Detection Strategy

- LightGBM classification model
- Optimized for **high recall**
- Probability-based decision threshold
- Combined multiple fraud signals:
  - Time
  - Transaction type
  - Amount
  - Balance behavior

Design Principle

- Catch maximum fraud with minimum impact on genuine users

04

IMPACT

Model Performance Summary

How Well Does the Model Perform?

- The model was tested on completely unseen validation data
- Real-world decision setup: ALLOW | BLOCK | REVIEW

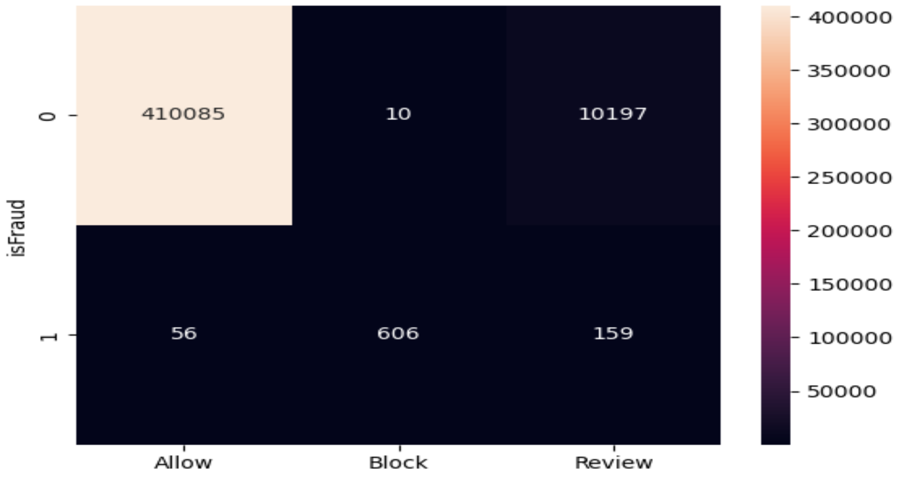
What we achieved?

- The model successfully detects more than 93% of fraud.
- Only ~7% fraud manages to pass through.
- Genuine transaction saved ~98%.
- Just ~2.5% transactions need manual review.

Why this matters?

- We are catching most fraud, without slowing down the system.

Decision Outcomes



What this tells us

- Fraud is **rarely allowed**
- Genuine users are **almost never blocked**
- Suspicious cases are **sensibly routed to review**
- Decisions look **practical, not aggressive**.

Fraud Handling Effectiveness

How Effectively Do We Stop Fraud?

- Total fraud cases: 821
- Stopped immediately (Blocked): 606
- Flagged for review: 159
- Missed fraud: only 56

In simple terms

- 93 out of every 100 frauds are intercepted
- Only a very small fraction slips through

What this means

The system does its core job well — stopping fraud before damage happens.

Genuine User Protection

How Well Are Genuine Users Protected?

- Only 10 genuine transactions were wrongly blocked
- Blocking precision: 98.4
- Most genuine users experience no interruption at all

Why this is important

- False blocks hurt trust
- This model avoids unnecessary friction
- Genuine users can transact freely, without fear of being wrongly stopped.

Operational Impact

Impact on Fraud Operations Team

- Only **~2.5% transactions** go to manual review
- Review queue stays **small and manageable**
- Team focuses on **real risk**, not noise

Operational reality

- Less alert fatigue
- Better use of human reviewers
- System remains scalable as volume grows

Overall Business Impact

Business Impact: Baseline vs Our Model

Performance Comparison :

Metric	Baseline System	Our Model
Fraud Recall	~0.2%	~93%
Fraud Leakage	~99.8%	~6–7%
Precision	Not meaningful	~98% (Blocking)
Review Load	0% (No review)	~2.5%
Automation Quality	100% wrong automation	Smart, selective automation

Overall Business Impact

What Changed Because of Our Model

- In the baseline system, almost all fraud passed through undetected, leading to direct financial loss.
- With our model:
  - More than 9 out of 10 fraud cases are now intercepted
  - Fraud leakage drops from ~100% to single digits

Instead of blindly allowing everything, the system now:

- Blocks confirmed fraud
- Reviews only suspicious cases
- Allows genuine users smoothly

Overall Business Impact

Why This Is a Big Business Win

- Fraud losses reduced drastically
- Genuine users protected from unnecessary disruption
- Only ~2.5% transactions need manual review
- Fraud detection becomes intelligent instead of reactive

“Compared to the baseline system, our model transforms fraud detection from a loss-making blind system into a controlled, intelligent, and business-safe solution.”