ARISTOVA

Bank Fraud Detection And Reconciliation

For Aristova Private Bank

Data analytical approach for a business oriented environment, Addressing critical business challenges, tackling current inefficiencies in detecting fraud, ensuring ledger accuracy and providing timely business insights.

Group Name: BrandStormers
Members: Shalom, Pranjal, Suhani, Sakshi

Batch Code: 06
Project Guide: Shivani Dangi

Introduction

ARISTOVA

- **Background of the project**

Aristova, a Chandigarh-based private bank, handles numerous daily financial transactions using a Master Ledger and a Simulated Ledger. The manual process of matching and checking these ledgers is time-consuming and often leads to missed transactions, incorrect transaction details, slow identification of potential fraud, and human effort.

- **Significance of the project**

❖ Enhances financial accuracy and trust by ensuring every rupee is accounted for, preventing losses and building trust.
❖ Facilitates rapid fraud detection by comparing transactions, allowing for quicker investigation and prevention of fraudulent activities.
❖ Provides significant efficiency gains by automating reconciliation, freeing up staff for strategic tasks.
❖ Provides clear insights for informed decision-making by providing dashboards on discrepancies and types of fraud.
❖ Ensures compliance by meeting strict regulatory and auditing requirements for financial reporting.

What does this project achieve?

- **Scope of work**

❖ Automating Reconciliation Process and Fraud Insights.

❖ Python program to read transaction data from Master and generate Simulated ledger for reconciliation process.

❖ Identifies matched, missing, and mismatched transactions.

❖ Interactive Power BI dashboard for reconciliation summary.

❖ Dedicated dashboard for analyzing fraudulent transactions.

❖ Both dashboards allow data filtering and exploration.

❖ Providing the Banking management and the software team with suitable and feasible recommendations based on our analysis.

Literature Review / Background Study

- **Review of existing solutions**

The Literature review explores four methods for detecting and analyzing fraud in financial systems: manual reconciliation, Commercial Off-the-Shelf (COTS) reconciliation software, stand-alone fraud detection systems, and basic scripting or database querying. Manual reconciliation has strengths like low setup costs but has limitations like scalability, time consumption, human error, and lack of real-time insight.

A background study reveals many existing systems struggle with efficient fraud detection, accurate reconciliation, and timely insights. This project aims to address these common gaps, enhancing financial integrity, reducing risk, and providing actionable intelligence through improved processes and automated alerts. Resources that assisted us throughout the project lifecycle includes articles, threads and explanatory videos on the web that help us understand the current scenario of the BFSI sector and particularly the banking industry.

- **Gaps identified**

❖ Addresses gap between reconciliation and fraud detection in traditional banking operations.
❖ Provides customization and agility with a custom Python script for reconciliation engine.
❖ Reduces manual processes and provides near real-time operational visibility.
❖ Leverages open-source Python and Power BI platform for cost-effectiveness.
❖ Provides limited actionable intelligence for investigators through interactive dashboards.

Problem Statement & Objectives

- **Clear statement of the problem**

Aristova Bank, a private banking institution in Chandigarh, currently struggles with a manual, time-consuming, and error-prone process for reconciling its high volume of daily transactions between its Master Ledger and the Fraud Detection System's Simulated Ledger. This disconnected and inefficient reconciliation not only leads to delayed identification and investigation of critical financial discrepancies (missing or mismatched transactions) but also significantly hinders the timely detection and analysis of potentially fraudulent activities, posing substantial financial and reputational risks to the bank.

The project's objective is to reduce fraud risk and improve ledger accuracy by detecting fraudulent transactions during reconciliation. It aims to identify fraud patterns, classify mismatches, and provide timely alerts for accurate reporting and efficient resolution, enhancing overall financial integrity. Streamlining the reconciliation procedure by identifying key performance metrics in our dataset, analyse them with the help of business analytical tools and come up with feasible yet effective recommendations to improve the bank’s internal reconciliation process.

Problem Statement & Objectives

- **Project objectives**

- Python-based system for automated ledger reconciliation and fraud analysis.
- Processes and compares transactions from Master and Simulated Ledgers.
- Integrates fraud flags from Simulated Ledger into core reconciliation process.
- Design Power BI dashboards for real-time reconciliation insights.
- Enhances operational efficiency by reducing manual effort.
- Empowers data analysts and fraud investigators with accessible data.
- Strengthens data integrity through consistent automated process.

Methodology / System Design

- **Tools & Technologies Used**

Excel: Primarily used for initial data analysis, small-scale data preparation, and documenting project aspects like requirements or test cases.

Power BI: Employed for visualizing complex fraud patterns, creating interactive dashboards, and presenting actionable insights derived from the reconciled ledger data.

Draw.io: Utilized as a versatile diagramming tool for designing and documenting various aspects of the system, including process flows, architecture, and other UML diagrams.

Python: Leveraged as a programming language for data manipulation, implementing core reconciliation logic, developing advanced fraud detection algorithms, and automating various system tasks.

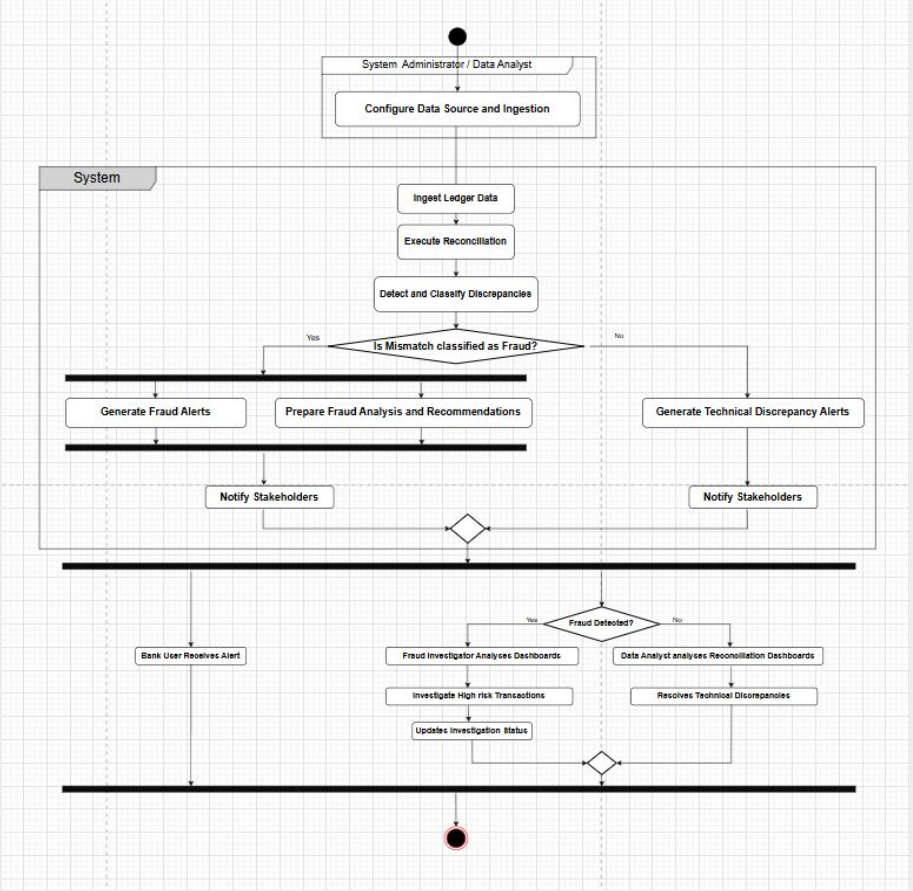
Methodology / System Design

- **Flowcharts, UML diagrams, architecture**

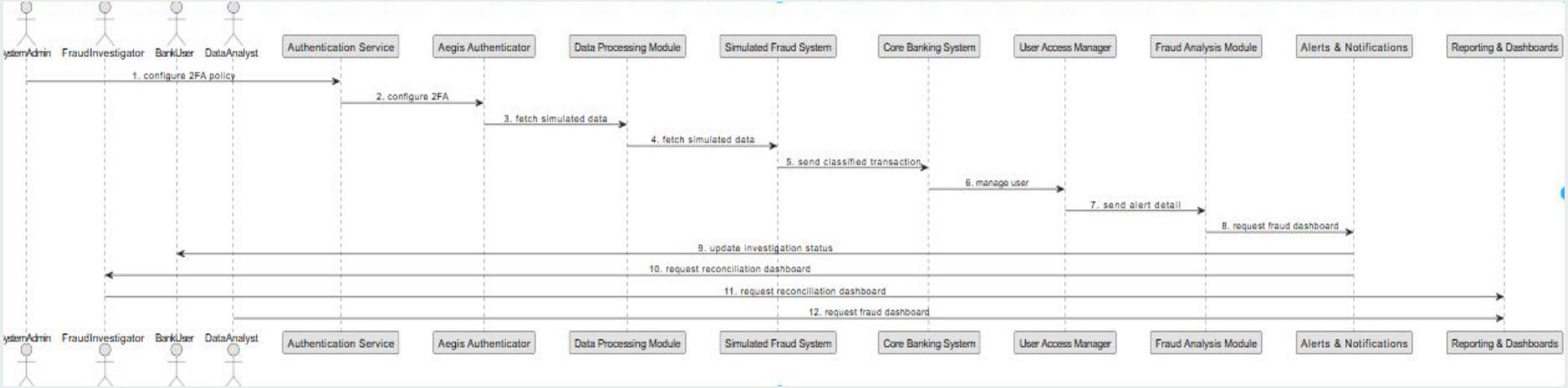
The following activity diagram showcases the flow of the reconciliation process in the banking system. It includes key stakeholders, Fraud investigators, business analysts.

The primary methods in this workflow includes executing reconciliation, detecting the discrepancies based off of primary indicators, and leveraging business tools to identify frequent patterns and insights for detecting of the discrepancy is a fraud or a technical inconsistency in the system.

The system also alerts the user (Customer) when a potential discrepancy occurs, or when high risk transactions are taking place

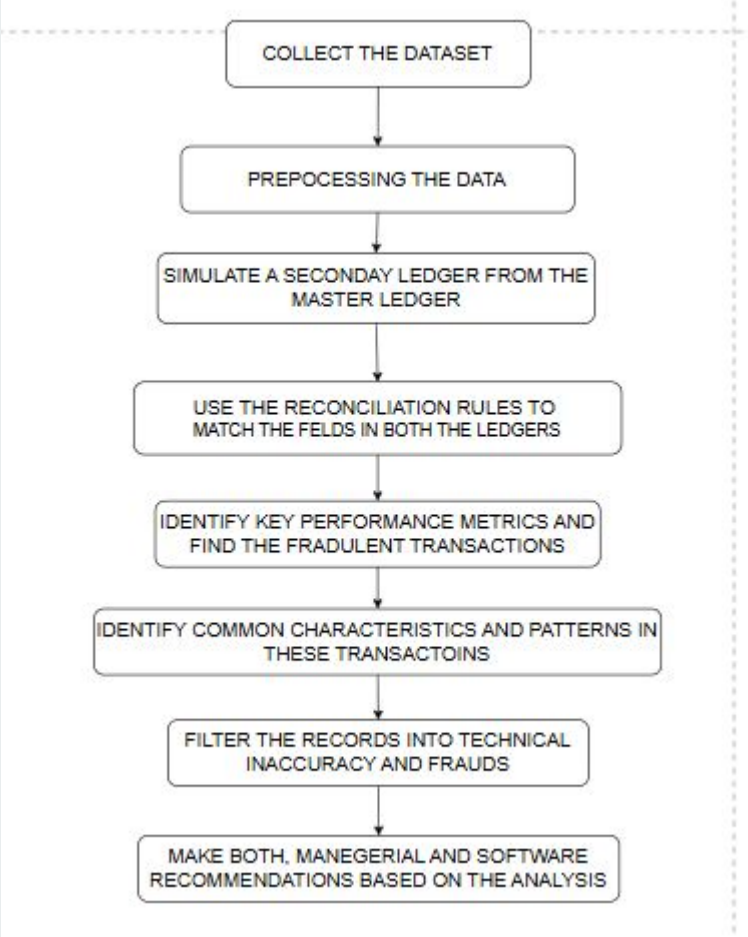


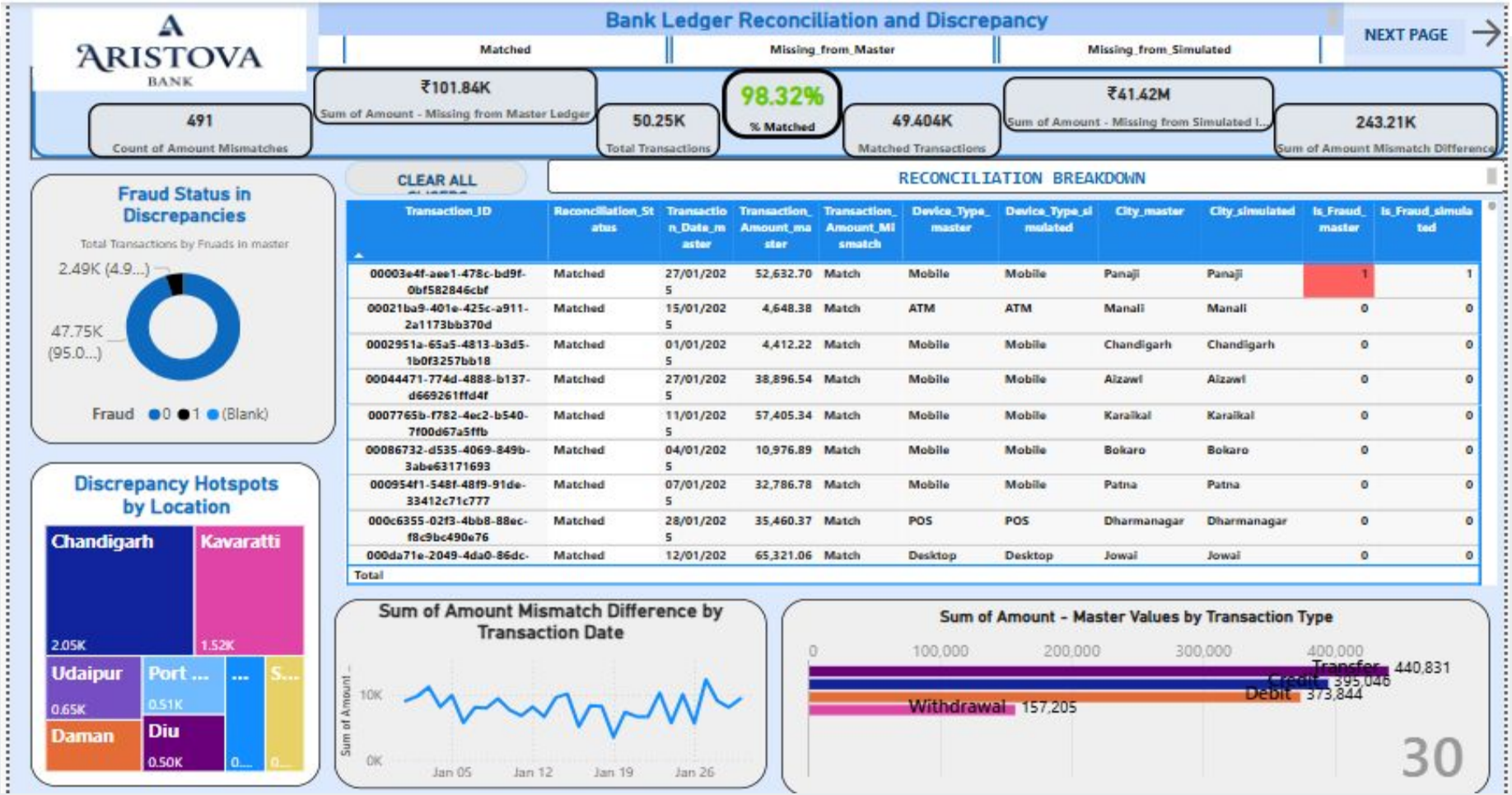
Sequence of Operations in the Reconciliation Process



Methodology / System Design

- **Phases of project development**




ARISTOVA BANK
Bank Ledger Reconciliation and Discrepancy
Matched
Missing_from_Master
Missing_from_Simulated
NEXT PAGE
₹101.84K
Sum of Amount - Missing from Master Ledger
98.32%
% Matched
₹41.42M
Sum of Amount - Missing from Simulated l...
491
Count of Amount Mismatches
50.25K
Total Transactions
49.404K
Matched Transactions
243.21K
Sum of Amount Mismatch Difference
Fraud Status in Discrepancies
Total Transactions by Fruads in master
2.49K (4.9...)
47.75K (95.0...)
Fraud 0 1 (Blank)
CLEAR ALL
RECONCILIATION BREAKDOWN
Transaction_ID
Reconciliation_Status
Transaction_Date_master
Transaction_Amount_master
Transaction_Amount_Mismatch
Device_Type_master
Device_Type_simulated
City_master
City_simulated
Is_Fraud_master
Is_Fraud_simulated
00003e4f-aee1-478c-bd9f-0bf582846cbf Matched 27/01/2025 52,632.70 Match Mobile Mobile Panaji Panaji 1 1
00021ba9-401e-425c-a911-2a1173bb370d Matched 15/01/2025 4,648.38 Match ATM ATM Manali Manali 0 0
0002951a-65a5-4813-b3d5-1b0f3257bb18 Matched 01/01/2025 4,412.22 Match Mobile Mobile Chandigarh Chandigarh 0 0
00044471-774d-4888-b137-d669261ffd4f Matched 27/01/2025 38,896.54 Match Mobile Mobile Aizawl Aizawl 0 0
0007765b-f782-4ec2-b540-7f00d67a5ffb Matched 11/01/2025 57,405.34 Match Mobile Mobile Karaikal Karaikal 0 0
00086732-d535-4069-849b-3abe63171693 Matched 04/01/2025 10,976.89 Match Mobile Mobile Bokaro Bokaro 0 0
000954f1-548f-48f9-91de-33412c71c777 Matched 07/01/2025 32,786.78 Match Mobile Mobile Patna Patna 0 0
000c6355-02f3-4bb8-88ec-f8c9bc490e76 Matched 28/01/2025 35,460.37 Match POS POS Dharmanagar Dharmanagar 0 0
000da71e-2049-4da0-86dc- Matched 12/01/202 65,321.06 Match Desktop Desktop Jowai Jowai 0 0
Total
Discrepancy Hotspots by Location
Chandigarh 2.05K
Kavaratti 1.52K
Udaipur 0.65K
Port ... 0.51K
Daman
Diu 0.50K
Sum of Amount Mismatch Difference by Transaction Date
Sum of Amount
10K
0K
Jan 05
Jan 12
Jan 19
Jan 26
Sum of Amount - Master Values by Transaction Type
0
100,000
200,000
300,000
400,000
Transfer 440,831
Credit 395,046
Debit 373,844
Withdrawal 157,205
30

FRAUDULENT TRANSACTION ANALYSIS

4.96%
% Fraudulent Transactions

₹ 124.20M
Total Fraudulent Amount

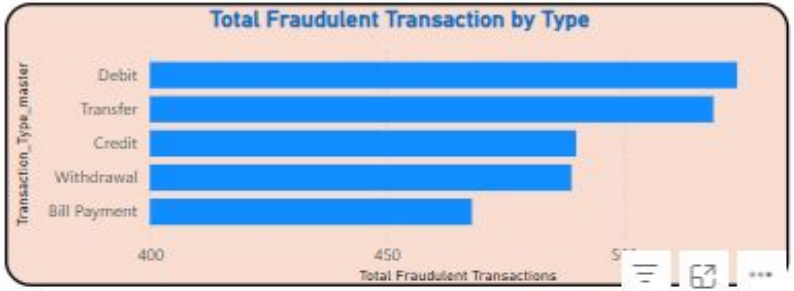
2490.0
Total Fraudulent Transactions

Fraud Status: (Blank) | 0 | 1

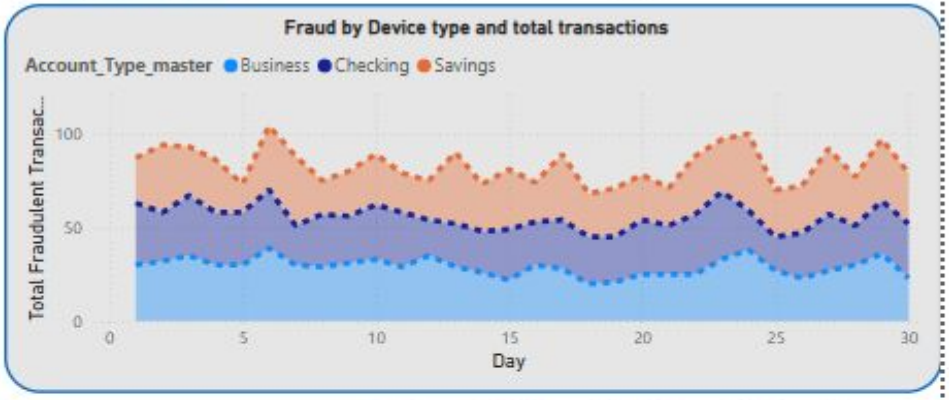
CLEAR ALL SLICERS

1/1/2025 — 1/30/2025

Total Fraudulent Transaction by Type



Fraud by Device type and total transactions



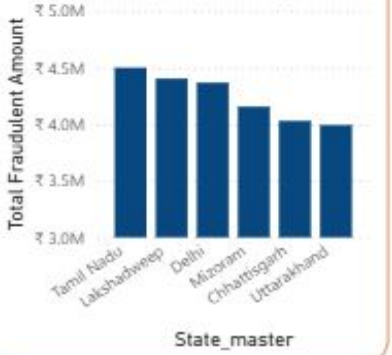
Transaction_Type_master	ATM	Desktop	Mobile	POS	Total
Bill Payment	128.0	118.0	116.0	106.0	468.0
Credit	110.0	135.0	117.0	128.0	490.0
Debit	134.0	109.0	136.0	145.0	524.0
Transfer	129.0	138.0	129.0	123.0	519.0
Withdrawal	107.0	137.0	117.0	128.0	489.0
Total	**608.0**	**637.0**	**615.0**	**630.0**	**2490.0**

4.96%
% Fraudulent Transacti...

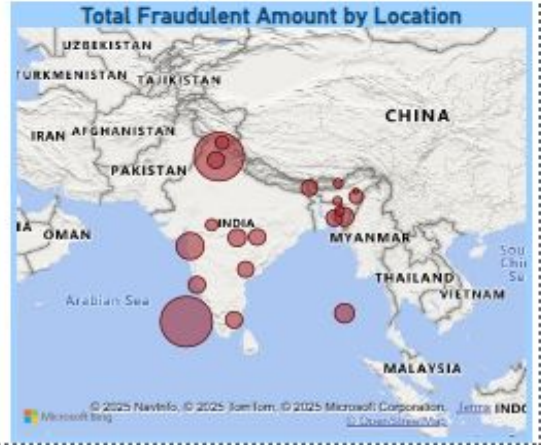
2490
Sum of Is_Fraud_master

2490.0
Total Fraudulent Trans...

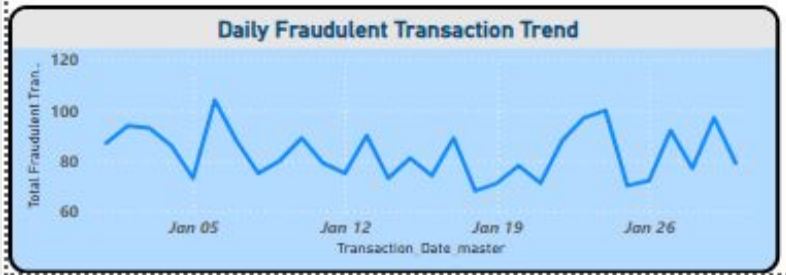
Total Fraudulent Amount by State_master



Total Fraudulent Amount by Location



Daily Fraudulent Transaction Trend



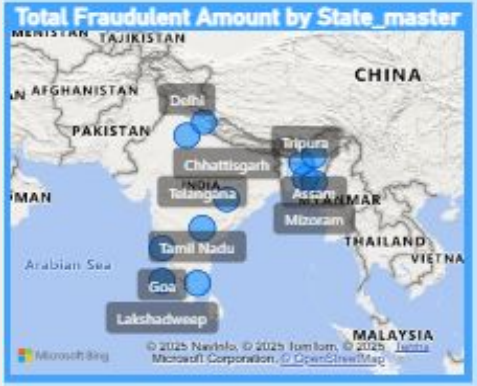
TRANSACTION DATES

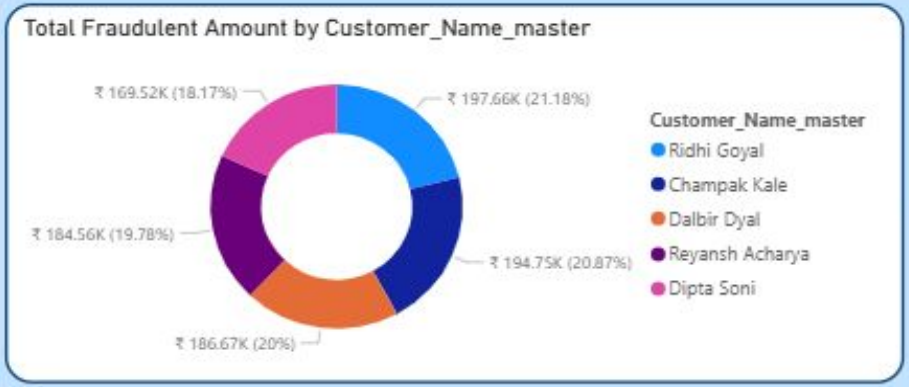
1 31

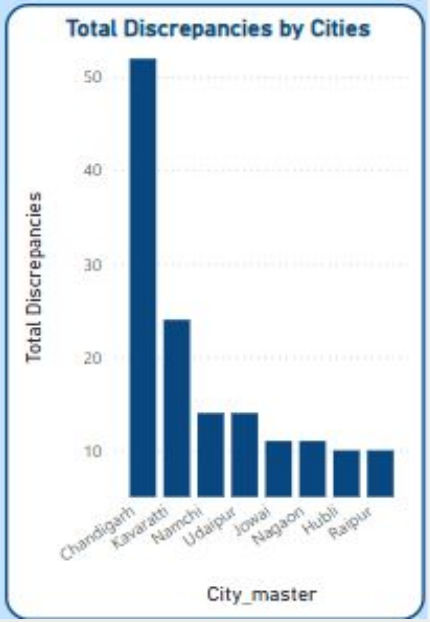
EXECUTIVE SUMMARY AND KEY TRENDS

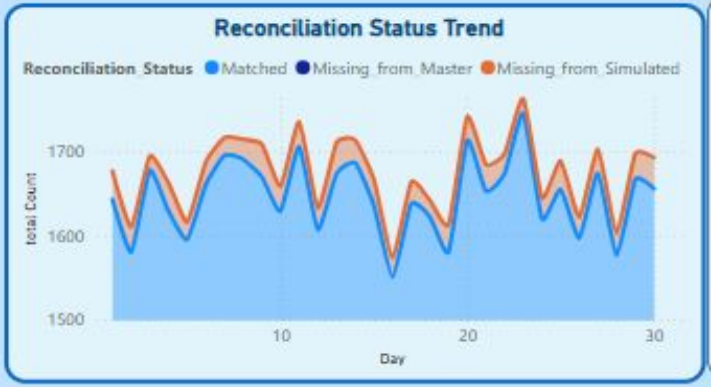
RESET ALL FILTERS

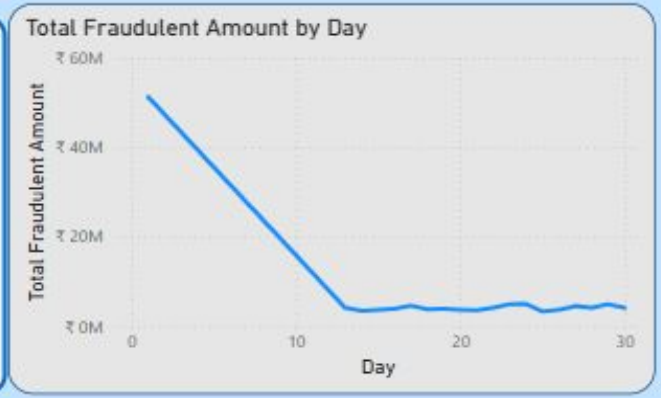
50246.00	98.32%	49404.000	2490.0
Total Transactions	% Matched	Matched Transactions	Total Fraudulent Transactions











Result and Analysis

- **Tables, charts, graphs for analysis**

MASTER LEDGER INSIGHTS

Count of Transaction_ID	transaction ty						
Recon status	Bill Payment	Credit	Debit	Transfer	Withdrawa	(blank)	Grand Total
Matched	9901	9903	9841	9924	9835		49404
Missing_from_Master						2	2
Missing_from_Simulated	160	169	189	162	160		840
Grand Total	**10061**	**10072**	**10030**	**10086**	**9995**	**2**	**50246**

What type of transactions were missing from the master ledger as compared to the simulated ledger? Also which transaction type is most seen across the data?

Count of Transaction_ID	Fraud status		
Device type (master)	0	1	Grand Total
ATM	12071	608	12679
Desktop	11905	637	12542
Mobile	11942	615	12557
POS	11836	630	12466
Grand Total	**47754**	**2490**	**50244**

It basically tells us which devices are generating more fraudulent transactions compared compared to other devices used for transactions, helping pinpoint fraud sources better!!

Result and Analysis

Count of Transaction_ID	reconciliation		
Date range	Matched	Missing_from_Simulated	Grand Total
1/1/2025 - 1/5/2025	8125	136	8261
1/6/2025 - 1/10/2025	8347	141	8488
1/11/2025 - 1/15/2025	8310	151	8461
1/16/2025 - 1/20/2025	8104	130	8234
1/21/2025 - 1/25/2025	8348	133	8481
1/26/2025 - 1/30/2025	8170	149	8319
Grand Total	**49404**	**840**	**50244**

Do you see the consistent number of 'Matched' transactions over time??

Is the pattern same for the transactions missing from the simulated ledgers? What does that hint to.

Summary of work done

- 1. Project & Data Foundation: Defined the project scope (Bank Ledger Reconciliation & Fraud Detection) and established an understanding of the key data attributes from master and simulated ledgers.
- 2. Core Reconciliation Logic: Outlined the Python-based logic for transaction matching and identifying various discrepancy types (e.g., missing, mismatched).
- 3. Power BI Data Modeling & Measures: Guided on loading combined data into Power BI and created essential DAX measures for total transactions, matched transactions, and detailed discrepancy counts/amounts.
- 4. Dashboard 1 - Reconciliation Overview: Designed and built the first dashboard, including primary KPIs, interactive slicers, detailed tables for discrepancies, and alternative visuals like Bar Charts and Treemaps.
- 5. Dashboard Functionality - Reset Button: Implemented a "Reset All Filters" button using Power BI bookmarks to enhance dashboard usability.
- 6. Dashboard 2 - Fraud Analysis Deep Dive: Initiated the second dashboard, setting up fraud-specific KPIs, a trend analysis line chart, and categorical breakdowns for fraud patterns.
- 7. UML & Role Definitions: Developed a Use Case Diagrams for system interactions and clearly defined the responsibilities of key project stakeholders (Fraud Investigator, Business Analyst, Bank User, Managing Director) for the BRD.

WHAT WERE OUR KEY TAKEAWAYS??

There is no master tool while working on our projects, What Excel could not do, python did!

Why use Power BI when we can make charts in Excels?

Should there be any changes in the management? Or is it just software?

Why did we need business analyst for this problem?

References for the project

- https://www.kaggle.com/datasets/marusagar/bank-transaction-fraud-detection
- https://cpl.thalesgroup.com/blog/access-management/digital-banking-fraud-prevention
- https://www.inkle.io/blog/bank-reconciliation-process
- https://www.bluecopa.com/blog/what-is-bank-reconciliation

THANK YOU