## Business Problem Statement

The bank operates in a digital environment where customers perform financial transactions across multiple channels, including mobile devices, desktop interfaces, and online banking platforms. With increasing transaction volume, the institution faces the challenge of maintaining secure, seamless, and real-time transaction processing while preventing financial fraud.

Fraudulent activities—such as unauthorized account access, abnormal transaction patterns, and misuse of network resources—pose a significant risk to revenue, customer trust, and the bank's regulatory compliance standing. The presence of the Fraud_Flag indicator in the dataset highlights that fraudulent transactions are actively occurring, and the bank requires a systematic approach to detect, analyze, and mitigate them.

Additionally, the dataset contains key network performance metrics such as Network Slice ID, Bandwidth (Mbps), and Latency (ms), which influence transaction success rates and user experience. Performance instability in certain network slices or bandwidth groups may contribute to failed transactions or create openings that fraudsters exploit.

Moreover, geolocation coordinates (Latitude and Longitude) provide insight into where transactions originate, enabling the identification of high-risk regions or suspicious geographic behavior such as unusual transaction clustering from unfamiliar locations.

Therefore, the bank needs a comprehensive business intelligence solution that monitors transaction trends, identifies fraud patterns, assesses system performance, and supports proactive fraud prevention strategies.

## Project Objective

This project aims to analyze bank transaction data to:

Measure overall transaction performance and highlight operational efficiency across transaction types, devices, timestamps, and network slices.

Identify and quantify fraudulent transactions, including total fraud counts, monetary impact, and fraud distribution across transaction types, devices, locations, and bandwidth groups.

Detect behavioral and temporal fraud trends, such as peak fraud hours or abnormal geolocation patterns.

Evaluate network performance factors (bandwidth and latency) to understand their impact on both successful and fraudulent transactions.

Provide drill-down transaction visibility that enables fraud teams and business analysts to trace individual suspicious transactions.

Support data-driven decision making, including:

Strengthening authentication controls for vulnerable devices.

Improving bandwidth allocation for high-risk slices.

Enhancing real-time fraud monitoring and flagging systems.

## Expected Business Impact

By implementing this analytics solution, the bank can:

Reduce financial losses by identifying fraud early.

Improve customer trust and transaction reliability.

Enhance regulatory compliance through transparent fraud monitoring.

Optimize digital banking infrastructure performance.

Strengthen operational awareness and strategic fraud response planning.

The results of this project will enable the bank to proactively safeguard assets, enhance platform security, and deliver a more resilient and trustworthy digital banking experience.

## Summary

This analysis provides actionable insights into transaction behaviors, fraud patterns, and network performance. It enables targeted security improvements, operational efficiency, and strategic fraud prevention initiatives that collectively reinforce the bank’s digital safety and customer confidence.