10Alytics

Specialization: *Fraud detection, banking.*

Business Focus: *Banking and Finance Industry*

Tool: *PostgreSQL*

BANK FRAUD DETECTION AND PREVENTION

Project Learning Opportunities

This case study will focus on detecting flagged transactions in a bank's transaction data using SQL queries

Tools and Technology to be Used

10Alytics

Case Study Overview

Introduction to the Business

PioneerTrust Bank is a financial institution serving millions of customers. As the bank expands its operations, it has noticed an increasing rate of flagged transactions involving accounts and credit card activity. These flagged activities lead to significant financial losses and have a major impact on customer trust. The bank aims to develop better fraud detection models to prevent future flagged activities and protect its customers

Case Study Overview

Problem Statement

PioneerTrust Bank is experiencing a rise in flagged transactions, resulting in financial losses. The current fraud detection system is not advanced enough to spot flagged activity in real-time, causing delayed responses to fraud alerts. The bank needs a more effective system that can analyze past transaction data to identify patterns indicative of fraud and prevent it in the future.

10Alytics

Rationale for the Project

1.

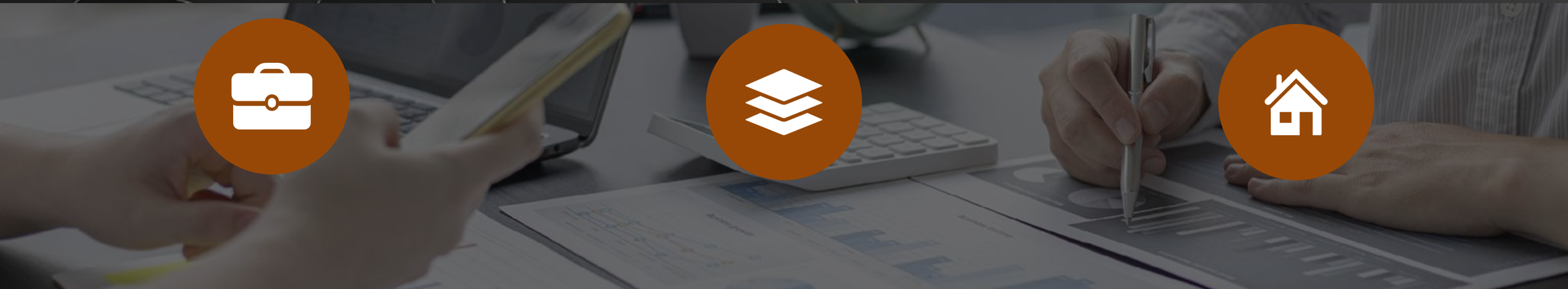
Improving fraud detection by analyzing transaction data with SQL to identify flagged activities, reducing financial losses, and protecting customers.

2.

Detecting and preventing fraud in real-time to protect customers, reduce financial losses, and enhance trust in the bank's security.

3.

Providing actionable insights through data analysis to enable the bank's fraud prevention team to make proactive, data-driven decisions.



10Alytics

Case Study Objectives

Identify High-Risk Transactions

Detect Patterns of flagged Behavior

Analyze Multiple Location Transactions

Evaluate Repeat Offenders and Recurring flagged Activities

Build Data-Driven Recommendations for Fraud Prevention

Gain Proficiency in SQL Data Analysis

10Alytics

Email From the Line Manager

Hello Analyst,

Following our recent meetings, the Data Engineering Team has completed the preparation of the data required for analyzing flagged transactions. The data has been loaded into our central database. We need your help analyzing this data to uncover any patterns or anomalies that could indicate fraud.

Here's what we need from you:

Use SQL to analyze transaction amounts, customer behavior, transaction locations, and account activities.

Focus on identifying high-risk transactions, particularly large transactions, unusual patterns, or activity outside normal operating hours.

Identify unusual spikes in transaction volume or multiple transactions from different locations for the same account.

The database is ready for analysis. Please let me know if you need any assistance with the data.

Best regards,
Stanley,
Line Manager.

10Alytics

Data Description

Transactions Table:

Contains transaction information such as transaction id, customer id, account id, amount, transaction date, merchant location, transaction type.

Each transaction may be flagged as flagged or legitimate.

Customers Table:

Stores customer information like customer id, name, location, and account type.

Accounts Table:

Contains account-specific data such as account id, account status, and creation date.

10Alytics

SQL Tailored Analysis Questions

High Transaction Amounts:

- What are the top 5 highest transaction amounts this month?
- What is the average transaction amount for all transactions this month?
- Are there transactions above the average limit?

Repeat Offenders:

- Are there customers that made more than 1 flagged transaction?...which customer has the highest flagged transactions?
- How many total flagged transactions occurred this month?...what dates has the most flagged activity?
- Are flagged transactions more likely to be deposits or withdrawals?

Transactions from Multiple Locations:

- Which customers have made transactions from more than 2 different locations in a single day?
- Which Location has the most flagged transactions?
- Which account is most associated with flagged transactions

10Alytics

Tech Stack

PostgreSQL

10Alytics

Project Workflow

PREPARATION

The data is cleaned, transformed, and loaded into the bank's central database. The data engineering team ensures that the tables are ready for analysis by data analysts.

ANALYSIS

Using SQL queries to identify high-value transactions, repeat offenders, and customers making transactions from multiple locations.

INSIGHT

Generate insights on fraud detection patterns using SQL. This may include identifying customers with multiple flagged transactions, detecting transactions from geographically distant locations, and reviewing high-value transactions.

RECOMMENDATIONS

Based on the analysis, the data analyst will provide actionable recommendations for improving the bank's fraud detection system, which may include setting up automated alerts for high-risk transactions.

10Alytics

Dataset

Click HERE to download the Database

10Alytics

READY TO DELVE IN?