BFSI AML & Fraud Detection System

1. Introduction

This document provides a comprehensive overview of the BFSI (Banking, Financial Services, and Insurance) Anti-Money Laundering (AML) and Fraud Detection system. The system is designed to detect suspicious transactions, monitor fraud patterns, and ensure compliance with AML/CFT regulations. It covers database structures, procedures, scheduled jobs, and workflows implemented in Oracle Database.

2. Database Schema

The following tables are created to support AML and fraud detection use cases. Each table serves a specific purpose within the system.

Table	Purpose
CUSTOMER	Stores customer KYC details including PEP and sanctions flags.
ACCOUNT	Holds customer account information and balances.
CORE_TRANSACTION	Core banking transactions with suspicious transaction flagging.
CARD_TXN	Card transactions including merchant details and fraud labels.
AML_ALERT	Central repository of alerts generated by detection procedures.
FRAUD_EVENTS	Stores detected fraud cases with severity and notes.
AUDIT_LOG	Captures all procedure execution and errors for audit trail.
PEP_SCREENING	PEP screening matches with resolution status.
SANCTIONS_MATCHES	Sanctions list matches with resolution status.
INSURANCE_POLICY	Insurance policy records per customer.
CLAIM	Insurance claim details.
LOAN	Loan issuance records.
LOAN_REPAYMENT	Loan repayment details.
MERCHANT	Merchant details including categories.

3. Sequences

Sequences are used to generate unique identifiers for key records.

SEQ_AUDIT	Generates IDs for audit logs.
SEQ_AML_ALERT	Generates IDs for AML alerts.

4. Stored Procedures

- PROC_DETECT_STRUCTURING - Detects structuring (smurfing) transactions.

- PROC_DETECT_CARD_HIGH_VALUE - Detects high-value card transactions as potential fraud.

- PROC_DETECT_RAPID_CREDIT_DEBIT - Detects rapid credits followed by immediate debits.

- PROC_DETECT_HIGH_RISK_GEO - Detects transactions involving high-risk geographies.

- PROC_DETECT_SANCTIONS - Matches customers against sanctions lists.

- PROC_DETECT_PEP - Detects politically exposed persons.

- PROC_UPDATE_ALERT_STATUS - Updates alert lifecycle status (OPEN, UNDER_REVIEW, ESCALATED, CLOSED).

5. Job Scheduling

JOB_STRUCTURING_DETECT	Runs PROC_DETECT_STRUCTURING at defined intervals.
JOB_CARD_HIGH_VALUE	Runs PROC_DETECT_CARD_HIGH_VALUE at defined intervals.
JOB_RAPID_CREDIT_DEBIT	Runs PROC_DETECT_RAPID_CREDIT_DEBIT at defined intervals.
JOB_HIGH_RISK_GEO	Runs PROC_DETECT_HIGH_RISK_GEO at defined intervals.
JOB_SANCTIONS_DETECT	Runs PROC_DETECT_SANCTIONS at defined intervals.
JOB_PEP_DETECT	Runs PROC_DETECT_PEP at defined intervals.

6. Audit & Logging

All detection procedures log their execution into AUDIT_LOG. The log contains the object name, action, action initiator, timestamp, and details (including error messages). This ensures full traceability for compliance and audit purposes.

7. Workflow

AML alerts follow a lifecycle managed through PROC_UPDATE_ALERT_STATUS. Statuses include OPEN, UNDER_REVIEW, ESCALATED, and CLOSED. Additional REVIEW_NOTES can be added for audit purposes.

8. Security & Best Practices

Role-based access controls must be implemented for users managing AML/Fraud procedures. KYC, PEP, and sanctions data must be handled as sensitive information. Audit trails must be preserved without tampering to meet compliance requirements.

9. Future Enhancements

Potential enhancements include API integration for external monitoring tools, dashboards for visualization, and machine learning models for anomaly detection.