USE CASE DIAGRAM

Core Digital Transformation for Retail Banking

Actors, Use Cases, and Detailed Flow Descriptions

Project Title	Core Digital Transformation for Retail Banking
Document Type	Use Case Diagram & Flow Descriptions
Date	February 18, 2026
Prepared By	Business Analyst / System Architect
Version	1.0 – Initial Release
Status	Draft – Pending Stakeholder Review

1. Objective

This document visualizes system interactions and responsibilities of different actors in the banking ecosystem. It identifies primary actors (customers, staff) and secondary actors (external systems, regulators) and maps their interactions with key use cases to clarify system boundaries, functional scope, and integration touchpoints.

2. Actors

2.1 Primary Actors

Primary actors are human users or internal systems that directly initiate interactions with the banking platform:

Actor Name	Type	Role in System
Customer	Primary	Retail banking customer who uses the system for onboarding, account management, and transactions
Product Owner	Primary	Business stakeholder who manages fraud rules, loan workflows, and compliance configurations
Compliance Officer	Primary	Monitors KYC/AML compliance, reviews audit logs, and accesses regulatory reports
DevOps Engineer	Primary	Manages CI/CD pipelines, deployments, monitoring, and infrastructure provisioning

2.2 Secondary Actors

Secondary actors are external systems, regulators, or APIs that are invoked by the system or provide data/services:

Actor Name	Type	Role in System
External Regulator	Secondary	Regulatory bodies (FCA, CFPB, PCI Council) that receive compliance reports and submissions

Actor Name	Type	Role in System
Credit Bureau API	Secondary	Third-party system providing credit scoring and bureau data integration
Payment Gateway	Secondary	External payment processing system for transaction routing and settlement
Fraud Detection Engine	Secondary	AI/ML-powered system that analyzes transaction patterns and generates alerts

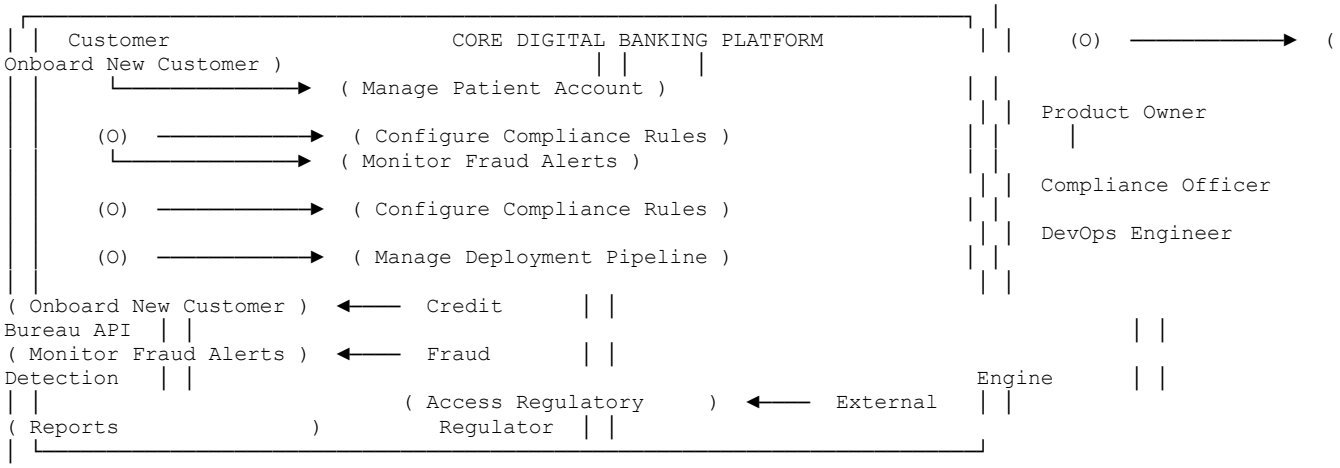
3. Use Cases

The following use cases represent the major functionalities the system must support. Each use case is described with its primary action and expected outcome:

Use Case Name	Description
Onboard New Customer	Customer submits KYC information, system verifies identity in real-time, account is created and activated within 5 minutes
Manage Patient Account	Customer views account statements, updates personal information, and configures notification preferences via self-service portal
Configure Compliance Rules	Compliance Officer defines AML thresholds, configures audit retention policies, and sets up automated regulatory report schedules
Manage Deployment Pipeline	DevOps Engineer configures CI/CD workflows, triggers builds/tests, and executes blue-green deployments with automated rollback
Monitor Fraud Alerts	Product Owner reviews real-time fraud alerts, adjusts detection rules, and manages investigation case workflows
Access Regulatory Reports	External Regulator receives automated compliance submissions including KYC reports, AML findings, and audit trail exports

4. Use Case Diagram Visualization

The diagram below represents the system boundary (Core Digital Banking Platform) with actors positioned outside the boundary and use cases inside. Lines connect actors to the use cases they interact with.



5. Actor-Use Case Relationships

5.1 Direct Interactions

- Customer → Onboard New Customer: Initiates the KYC onboarding flow and submits identity verification documents
- Customer → Manage Patient Account: Accesses self-service portal for account updates and statement retrieval
- Product Owner → Configure Compliance Rules: Defines AML thresholds and audit retention policies
- Product Owner → Monitor Fraud Alerts: Reviews and adjusts fraud detection rules in real-time
- Compliance Officer → Configure Compliance Rules: Sets regulatory report schedules and compliance parameters
- DevOps Engineer → Manage Deployment Pipeline: Executes CI/CD workflows and monitors deployment health

5.2 System-to-System Interactions (Secondary Actors)

- Credit Bureau API → Onboard New Customer: Invoked during onboarding to verify credit history and identity
- Fraud Detection Engine → Monitor Fraud Alerts: Analyzes transaction patterns and generates real-time alerts
- Payment Gateway → (implicit): Processes payment transactions initiated by customers
- External Regulator → Access Regulatory Reports: Receives automated compliance submissions and audit exports

6. Detailed Flow Descriptions

Use Case: Onboard New Customer

Precondition: Customer has valid identity documents (passport, driver's license, or national ID)

Main Flow:

- Customer navigates to the onboarding portal (web or mobile app)
- System presents KYC data collection form (name, address, DOB, ID number)
- Customer uploads identity verification documents (passport scan, proof of address)
- System validates document formats and performs OCR extraction
- System invokes Credit Bureau API to verify identity and credit history
- System performs AML screening against watchlists and sanctions databases
- If all checks pass, system creates customer account and assigns account number
- System sends confirmation email/SMS with account credentials

Postcondition: Customer account is active and ready for transactions. Onboarding completed in under 5 minutes.

Alternative Flow: If identity verification fails, system prompts customer to re-upload documents or contact support.

Use Case: Configure Compliance Rules

Precondition: Compliance Officer has admin-level access to the compliance dashboard

Main Flow:

- Compliance Officer logs into the compliance dashboard with MFA authentication
- Officer navigates to AML Rules Configuration section
- Officer defines transaction thresholds (e.g., flag transactions > $10,000)
- Officer configures automated reporting schedules (daily, weekly, monthly)
- System validates rule logic and checks for conflicts with existing rules
- Officer reviews and approves rule changes
- System activates new rules and logs configuration change in audit trail

- System sends confirmation notification to Officer and audit team

Postcondition: New compliance rules are live and applied to all incoming transactions.

Alternative Flow: If rule conflicts are detected, system alerts Officer and blocks activation until conflicts are resolved.

Use Case: Manage Deployment Pipeline

Precondition: DevOps Engineer has access to CI/CD platform and code repository

Main Flow:

- DevOps Engineer commits code changes to version control (Git)
- CI/CD platform detects commit and triggers automated build process
- System runs unit tests, integration tests, and security scans
- If all tests pass, system packages application into container image
- Engineer selects deployment strategy (blue-green or canary)
- System deploys to staging environment for UAT validation
- After UAT sign-off, Engineer approves production deployment
- System executes deployment with automated health checks
- If health checks fail, system triggers automatic rollback within 2 minutes
- System logs deployment event and notifies stakeholders of completion status

Postcondition: New application version is live in production with zero downtime.

Alternative Flow: If automated tests fail, deployment is blocked and Engineer receives failure report with logs.

Use Case: Monitor Fraud Alerts

Precondition: Fraud Detection Engine is operational and analyzing transaction streams in real-time

Main Flow:

- Fraud Detection Engine continuously analyzes transaction patterns using ML models
- When suspicious pattern is detected, Engine generates alert within 30 seconds
- Alert is routed to Product Owner's fraud monitoring dashboard
- Product Owner reviews alert details (transaction amount, location, account history)
- Owner investigates customer account activity and transaction context
- Owner decides to: (a) approve transaction, (b) block transaction, or (c) escalate to compliance
- System executes Owner's decision and updates fraud case status
- System captures investigation notes and evidence in case management workflow
- All actions are logged in audit trail with timestamp and user attribution

Postcondition: Fraud case is resolved and customer account status is updated accordingly.

Alternative Flow: If alert is false positive, Owner adjusts detection rules to reduce future false positives.

7. Reflection Questions

What challenges did you face in defining actors and use cases?

The main challenge was balancing granularity — deciding whether to model high-level business processes or break them into atomic use cases. For example, 'Onboard New Customer' encompasses multiple sub-processes (identity verification, credit check, AML screening) that could each be separate use cases. We opted for a business-oriented approach that groups related steps into meaningful outcomes, making the diagram more accessible to non-technical stakeholders.

How does the use case diagram clarify system boundaries?

The diagram explicitly shows what is inside the 'Core Digital Banking Platform' boundary (the use cases) versus what is outside (actors). This helps stakeholders understand that external systems like Credit Bureau APIs and

regulators interact with the platform but are not part of the platform itself. It also clarifies that customers and staff are users of the system, not components within it.

What improvements could enhance system interactions?

Future enhancements could include: (1) Adding <<include>> and <<extend>> relationships to show use case dependencies (e.g., 'Verify Identity' is included in 'Onboard New Customer'); (2) Modeling exception handling flows more explicitly; (3) Incorporating time-based triggers (e.g., scheduled batch jobs for regulatory reporting); (4) Adding swimlane diagrams to show cross-functional handoffs between Product Owners, DevOps, and Compliance teams during complex workflows like fraud investigation or incident response.