Part 1: Functional Baseline FFDB   
 **Mobile Payment App**

System Description:

The mobile payment app facilitates digital transactions between users, vendors, and financial institutions. It allows users to make payments, transfer funds, and manage their finances conveniently through their mobile devices.

**Functional Decomposition:**

**User Interface Management:**

Login/Registration: Allows users to create accounts or log in securely to access the app's features.

Profile Management: Enables users to update personal information, manage preferences, and view account details.

Transaction History: Provides a comprehensive record of past transactions for reference and tracking purposes.

Settings: Allows users to customize app settings, such as language preferences, notification preferences, and security settings.

**Payment Processing:**

Authentication: Verifies user identity through credentials or biometric authentication methods to ensure secure access.

Authorization: Validates payment requests and ensures users have sufficient funds or credit limits to proceed with transactions.

Transaction Verification: Confirms the authenticity and validity of transactions before processing them further.

Payment Confirmation: Provides users with confirmation notifications upon successful completion of payments, instilling trust and transparency in the process.

**Funds Transfer:**

Bank Account Linking: Allows users to link their bank accounts securely to the app for seamless fund transfers.

Fund Transfer Authorization: Validates fund transfer requests and ensures compliance with user-defined authorization protocols.

Transaction Verification: Verifies the accuracy and legitimacy of fund transfer requests to prevent errors or fraudulent activities.

Transfer Confirmation: Notifies users upon successful completion of fund transfers, providing reassurance and clarity regarding transaction status.

**Security and Fraud Prevention:**

Data Encryption: Utilizes robust encryption algorithms to safeguard sensitive user data and financial information from unauthorized access or breaches.

Biometric Authentication: Implements biometric authentication methods such as fingerprint or facial recognition to enhance security and prevent unauthorized access.

Transaction Monitoring: Constantly monitors transactions for suspicious activities or anomalies, triggering alerts for further investigation.

Fraud Detection: Utilizes advanced fraud detection algorithms to identify and mitigate fraudulent transactions, protecting users from financial losses and unauthorized transactions.

**Notification and Alerts:**

Transaction Notifications: Sends real-time notifications to users for every transaction, providing instant updates on their financial activities.

Account Alerts: Alerts users about account-related activities such as account balance updates, account login attempts, or suspicious activities.

Security Alerts: Notifies users about potential security threats or breaches, prompting them to take necessary precautions to safeguard their accounts and personal information.

**Integration with Financial Institutions:**

API Integration: Integrates with financial institution APIs to facilitate seamless communication and data exchange for transaction processing and account management.

Bank Communication: Establishes secure communication channels with partner banks for fund transfers, account verification, and transaction processing.

Financial Data Exchange: Enables exchange of financial data between the app and financial institutions for account synchronization, transaction reconciliation, and reporting purposes.

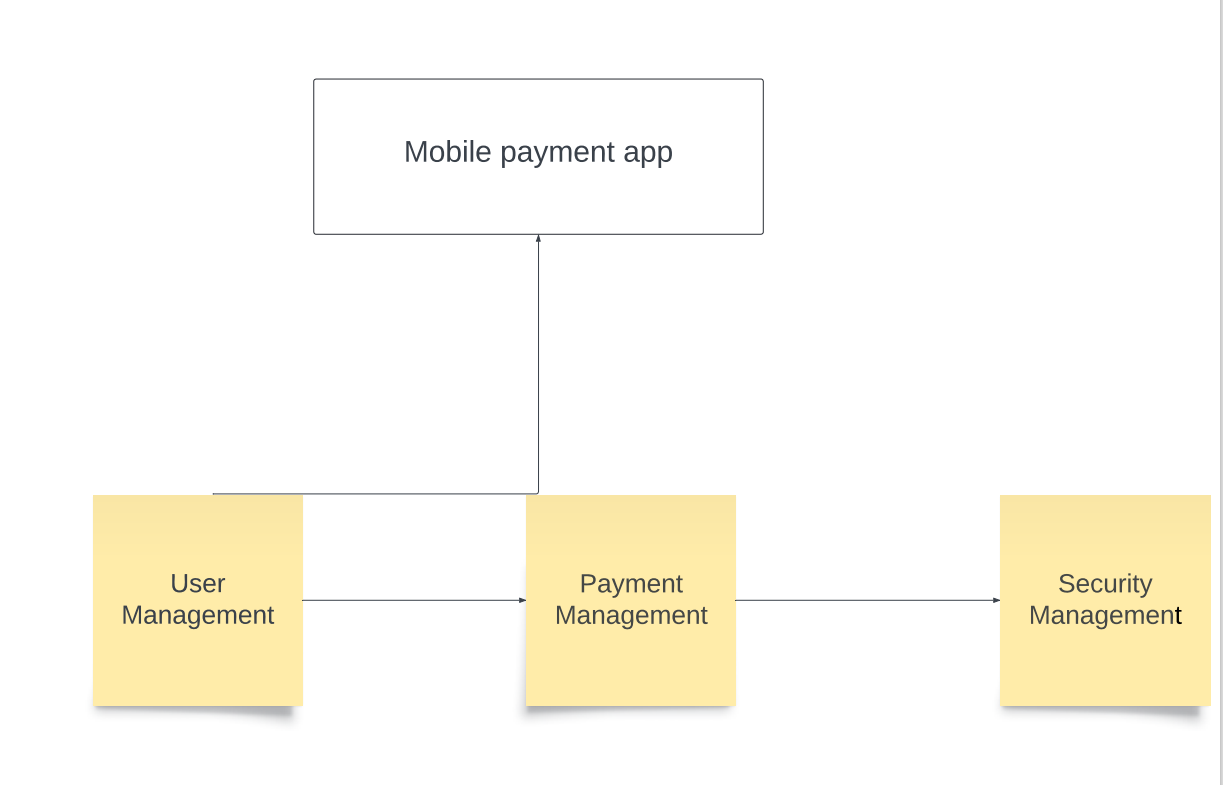
**Customer Support:**

Help Center: Provides users with access to comprehensive guides, FAQs, and troubleshooting resources to address common queries or issues.

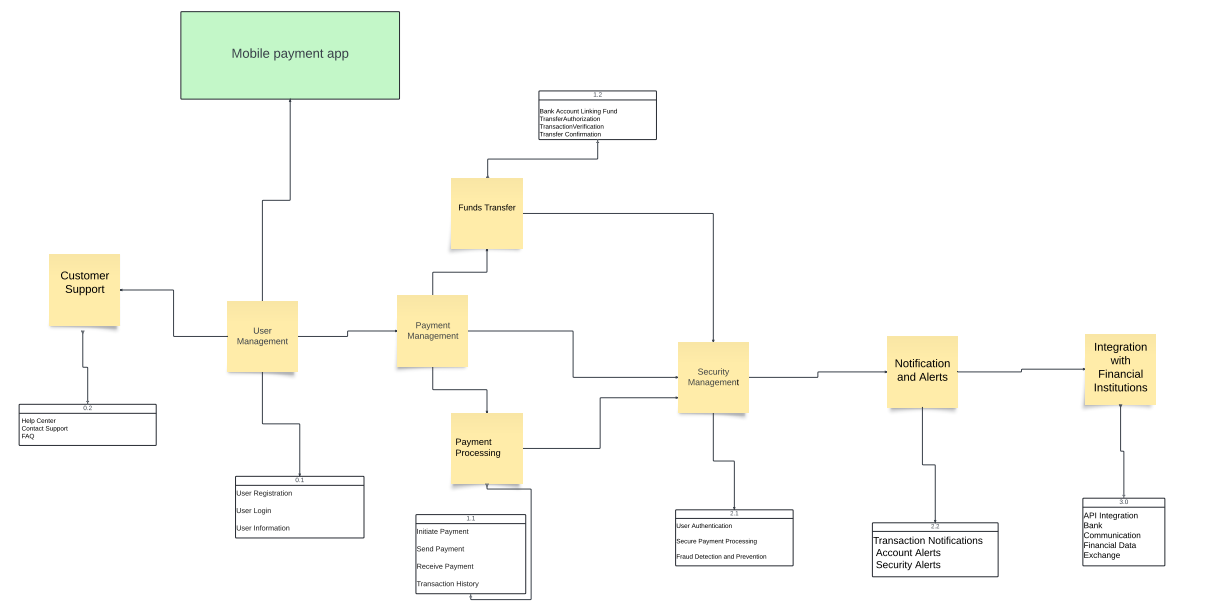
Contact Support: Allows users to contact customer support representatives directly for personalized assistance or resolution of complex issues.

FAQ: Offers a repository of frequently asked questions and answers to help users navigate the app's features and functionalities independently.

Functional Flow Block Diagram (FFBD):  
(A)



(B)



Part 2: Concept Comparison

## **Concept Sketch: Payment Processing System**

In the concept comparison phase, we aim to explore different technological concepts for a key functional block of the mobile payment app. Let's focus on the "Payment Processing" function, which is fundamental to the app's operation. We'll examine various technology concepts to enhance this function and provide users with secure and efficient payment processing capabilities.

## ****This sketch depicts the entire system flow, encompassing both NFC and QR code payment options.****

****Central Point:**** A central server facilitates communication between all components.  
****Customer:****Carries a smartphone with an NFC chip and a mobile wallet app.

****Vendor:****Possesses an NFC-enabled payment terminal and a QR code generator.

****Payment Process:****

****Customer Initiates Payment:****

Option 1 (NFC): Customer holds their phone near the NFC terminal.

Option 2 (QR Code): Customer opens their mobile wallet app and selects "Pay with QR Code." The app displays a unique QR code.

****Transaction Information Sent:****

Both options: The mobile wallet app transmits encrypted payment information (amount, account details) to the central server.

****Authorization Request:****

Central server: Verifies customer information and funds availability with the issuing bank.

****Authorization Response:****

Central server: Sends an authorization response back to the mobile wallet app (approved or declined).

****Payment Confirmation (NFC):****

If approved (NFC): The mobile wallet app displays a confirmation message on the customer's phone. The NFC terminal might also provide a visual or audible confirmation.

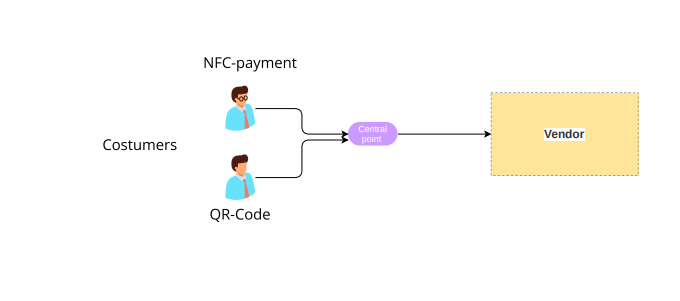
****Payment Confirmation (QR Code):****

If approved (QR Code): The vendor scans the QR code displayed on the customer's phone using their device or a dedicated QR code scanner app.

****Funds Transfer:****

Central server: Facilitates the transfer of funds from the customer's account to the vendor's account.

****Receipt (Optional):****

The mobile wallet app or vendor's system might display or print a receipt for the transaction.  
Concept Sketch:  
  
****Sketch Breakdown:****

****Left Side:**** Customer holding a smartphone near an NFC terminal (Option 1).

****Right Side:**** Customer phone displaying a QR code, being scanned by a vendor's device (Option 2).

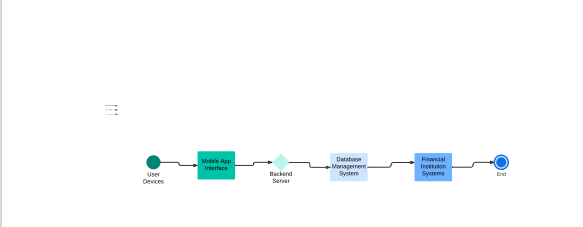
****Top Center:**** Central server connected to both customer and vendor systems.

****Arrows:**** Illustrate data flow between components.

**Part 3: System Architecture**

In this section, we'll outline the system architecture for the mobile payment app based on the chosen concept from Part 2. We'll provide a system architecture diagram, a physical baseline, and a functional allocation table to illustrate the structure and allocation of functions within the system.

**System Architecture Diagram:**



Physical Baseline:

1. Mobile App Interface

2. Backend Server

3. Database Management System

4. Financial Institution Integration

User Devices: Represented as smartphones or tablets, indicating the end-users accessing the mobile payment app.

Mobile App Interface:

Represents the graphical user interface (GUI) of the mobile payment app that users interact with.

Backend Server:

Central component responsible for processing transactions, managing user accounts, and communicating with external systems.

Database Management System: Stores user data, transaction history, and other relevant information securely.

Financial Institution Systems: External systems representing banks, payment processors, and other financial entities integrated with the mobile payment app.

Functional Allocation:

| **Function** | **Subsystem** |
| --- | --- |
| User Interface Management | Mobile App Interface |
| Payment Processing | Backend Server |
| Funds Transfer | Backend Server |
| Security and Fraud Prevention | Security Infrastructure |
| Notification and Alerts | Mobile App Interface |
| Integration with Financial Institutions | Backend Server |
| Customer Support | Backend Server |

**Recommendation:**

Based on the concept comparison and system architecture, it is recommended to prioritize the implementation of both NFC and QR code payment options to cater to a wider range of user preferences and technological capabilities. Additionally, ensuring robust security measures and seamless integration with financial institutions are crucial for the success and trustworthiness of the mobile payment app.