Project Design Phase-II
Proposed Solution Template

Date	October 16, 2023
Team ID	Team-591008
Project Name	Money Matters
Maximum Marks	2 Marks

Functional Requirements:

Following are the functional requirements of the proposed solutions

FR NO.	Functional requirements	Sub Requirement(Story/Sub-Task)
1.	**User Registration and Authentication:**	• User registration with email and password. • Two-factor authentication (2FA) for added security. • Password reset functionality.
2.	**Account Management:**	• Ability to create multiple accounts (savings, checking, credit card, etc.). • View and edit account details. • Close or freeze accounts.
3.	**Transaction Management:**	• Record and categorize income and expenses. • Schedule recurring transactions. • Generate transaction history and statements.
4.	**Budgeting and Financial Planning:**	• Set up budgets and financial goals. • Track progress toward financial goals. • Receive alerts or notifications for budget overages.
5.	**Investment and Asset Tracking:**	• Monitor and manage investments (stocks, bonds, mutual funds, etc.). • Track the value of assets like real estate or collectibles. • Provide investment insights and analytics.
6.	**Security and Privacy:**	• Implement strong encryption for data at rest and in transit. • Regular security audits and vulnerability assessments. • Privacy settings and consent management for user data.

Non-functional requirements:

Following are the non-functional requirements of the proposed solution

FR NO	Non-Functional requirements	Description
1.	Usability	• The application should have an intuitive and user-friendly interface to ensure users can easily navigate and perform financial tasks. • Usability testing to validate that users can complete tasks efficiently and without errors.
2.	Security	• Implement strong authentication mechanisms, including multi-factor authentication, to protect user accounts. • Encrypt sensitive user data (e.g., financial transactions, personal information) both in transit and at rest. • Regular security assessments and updates to protect against vulnerabilities and threats. • Compliance with industry-specific security standards and regulations (e.g., PCI DSS for credit card data).
3.	Reliability	• Ensure the system is highly reliable, minimizing downtime and errors. • Implement backup and disaster recovery solutions to prevent data loss in case of system failures. • Monitoring and error handling to detect and recover from failures automatically.
4.	Performance	• Ensure that the system responds promptly to user requests and maintains acceptable response times, even during peak usage. • Conduct performance testing to determine system bottlenecks and optimize system components as needed.
5.	Availability	• Maintain high availability to provide uninterrupted access to the service. • Implement redundancy and failover mechanisms to minimize service downtime. • Perform routine maintenance during non-peak hours to minimize user impact.
6.	Scalability	• Design the system to handle an increasing number of users and data without significant performance degradation. • Implement load balancing and horizontal scaling to distribute traffic efficiently. • Periodically assess and adjust scalability measures based on user growth.