**Usability Requirements:**

- The user interface should be intuitive and easy to navigate to ensure a positive user experience.
- Users should be able to perform basic tasks (e.g., creating a group, initiating a split) within 1 minute of interaction with the user interface.
- User satisfaction surveys should indicate an average satisfaction score of at least 4 out of 5.

**Performance Requirements:**

- The system should provide a responsive user interface, with pages loading within 2 seconds under typical user loads.
- The software should be capable of handling concurrent user loads of up to 1000 users without any request response time exceeding 3 seconds.
- Backend server response time for split requests and expense updates should be less than 100 milliseconds.

**Space Requirements:**

- The software should efficiently manage and store user data, ensuring that the database storage requirements are optimized.
- The database should support a minimum of 100,000 user accounts and associated transaction records.
- Data storage should not exceed 1 GB for every 10,000 user accounts.

**Security Requirements:**

- User data, including personal and financial information, should be encrypted both in transit and at rest.
- All data in transit should be encrypted using industry-standard TLS protocols.
- Data at rest should be encrypted using AES-256 encryption.
- Access control and authentication mechanisms should be in place to prevent unauthorized access to user accounts.
- Multi-factor authentication (MFA) should be enforced for all user accounts.
- Failed login attempts should trigger account lockouts for a defined period.
- The software should have mechanisms to detect and respond to security threats, such as intrusion detection and prevention systems.
- Intrusion attempts should be logged, and security alerts should be generated for the operations team.
- Regular security audits and updates should be performed to address vulnerabilities and compliance with security standards.
- Security audits should be conducted quarterly, and patches for critical vulnerabilities should be applied within 30 days of release.

**Environmental Requirements:**

- The software should be designed to work in various network environments, including mobile data and Wi-Fi.
- It should be compatible with a wide range of devices, including smartphones, tablets, and computers.

**Operational Requirements:**

- The software should have high availability, with a target uptime of 99.9%.
- The service should be available 99.9% of the time (approximately 8 hours and 45 minutes of downtime per year).
- The system should be easy to maintain and update without significant downtime.

- Software updates should be deployed during off-peak hours, with scheduled maintenance windows limited to 2 hours.

**Development Requirements:**

- The software development process should adhere to coding and testing standards.
- Version control and collaborative development tools should be in place.
- Adequate documentation for the software architecture and codebase should be maintained.
- The development team should follow secure coding practices to mitigate vulnerabilities.

**Regulatory Requirements:**

- The software should adhere to data privacy regulations, such as GDPR or HIPAA, depending on the user data handled.
- User data should be anonymized or pseudonymized to comply with GDPR data protection requirements.
- Compliance with financial regulations and payment processing standards should be maintained if financial transactions are involved.
- All financial transactions must adhere to PCI DSS compliance standards.

**Ethical Requirements:**

- The software should prioritize user privacy and data protection, and user consent should be obtained for any data processing.
- The system should discourage unethical financial practices or encourage fair expense sharing.

**Accounting Requirements:**

- If the software handles financial transactions, it should provide accurate and auditable financial records.
- Users should be able to view their transaction history, including payments and expenses.

**Safety/Security Requirements:**

- The system should implement security measures to protect against fraudulent activities.
- Safety measures should be in place to prevent accidental financial transactions or data loss.