项目文档

# Functional Requirement

ID Function Requirement  
AC-001 Account Creation The system shall allow users to create an account using a simple form that requires only basic information: email, password, and an optional username.  
AC-002 Account Creation The system shall support third-party sign-in options, such as Google and Apple, for account creation.  
AC-003 Account Creation Upon account creation, the system shall validate the email and send a confirmation link to activate the account.  
PM-001 Payment Management The system shall securely store payment methods with a user-controlled toggle labeled “Save for future purchases”.  
PM-002 Payment Management When a user proceeds to checkout and adds a new payment method, the system shall prompt them to confirm whether the method should be saved for future use.  
PM-003 Payment Management The system shall prompt users to update expiring payment cards during checkout.  
PM-004 Payment Management The system shall provide a dedicated section in account settings for managing saved payment methods, including editing and deleting.  
DM-001 Dispute Management The system shall provide a “Dispute” button for each transaction in the payment history.  
DM-002 Dispute Management The system shall allow users to submit a dispute form that includes a reason for the dispute and the ability to upload supporting documents.  
DM-003 Dispute Management The system shall provide real-time status tracking for submitted disputes, including updates on resolution progress.  
HP-001 Historical Payment Data The system shall allow users to access historical payment data via a dashboard or a search feature.  
HP-002 Historical Payment Data The system shall support filtering of payment history by date, merchant name, and transaction type.  
HP-003 Historical Payment Data The system shall allow users to export filtered or full payment data in CSV and PDF formats.  
IV-001 Identity Verification The system shall require re-authentication (e.g., 2FA via SMS or app) when users edit or delete payment methods.  
IV-002 Identity Verification The system shall support biometric verification (e.g., fingerprint or facial recognition) for high-risk actions such as accessing payment history or initiating disputes.  
IV-003 Identity Verification Re-authentication shall be adaptive and may be skipped for trusted devices.  
UC-001 User Control The system shall allow users to track or limit access permissions for shared accounts.  
UC-002 User Control The system shall clearly indicate which users can view or modify specific data in shared account scenarios.

# External Description

## 5.1 Regulatory/Legal Constraints  
  
- \*\*C-REG-001\*\*: The system shall comply with all applicable data protection regulations, including but not limited to the General Data Protection Regulation (GDPR) for European Union users and the California Consumer Privacy Act (CCPA) for users in California.   
 \*Priority: Must Have\*   
 \*Rationale: Legal compliance is essential to avoid penalties and maintain user trust.\*   
 \*Source: SRL-7\*   
 \*Acceptance Criteria: The system must pass a legal audit and demonstrate data protection practices in accordance with GDPR and CCPA.\*  
  
- \*\*C-REG-002\*\*: The system shall ensure that all financial data handling adheres to Payment Card Industry Data Security Standard (PCI DSS) Level 1 compliance.   
 \*Priority: Must Have\*   
 \*Rationale: Handling payment data requires strict adherence to industry security standards.\*   
 \*Source: NFR-2\*   
 \*Acceptance Criteria: The system must pass a PCI DSS Level 1 audit and demonstrate secure storage and transmission of payment data.\*  
  
- \*\*C-REG-003\*\*: The system shall not store raw or unencrypted credit card data beyond the scope of required payment processing.   
 \*Priority: Should Have\*   
 \*Rationale: Reducing the risk of data breaches by limiting the exposure of sensitive financial information.\*   
 \*Source: NFR-2\*   
 \*Acceptance Criteria: All credit card data shall be tokenized or encrypted using industry-standard algorithms.\*  
  
## 5.2 Hardware Constraints  
  
- \*\*C-HW-001\*\*: The system shall operate on standard web and mobile client hardware, including desktops, laptops, and smartphones.   
 \*Priority: Should Have\*   
 \*Rationale: Ensures broad accessibility across a wide range of devices used by customers and admins.\*   
 \*Source: SRL-5.1\*   
 \*Acceptance Criteria: The system shall be tested and validated for performance on the following hardware: Intel i5 or equivalent CPU, 8 GB RAM, and mobile devices with at least 2 GB RAM.\*  
  
- \*\*C-HW-002\*\*: The system shall be compatible with the latest versions of major web browsers (Chrome, Firefox, Safari, Edge) and mobile platforms (iOS 14+, Android 10+).   
 \*Priority: Must Have\*   
 \*Rationale: Maintains compatibility with the most widely used platforms to support all user classes.\*   
 \*Source: SRL-5.1\*   
 \*Acceptance Criteria: The system shall be verified for correct functionality and UI rendering on all specified client-side platforms.\*  
  
## 5.3 Interface Constraints  
  
- \*\*C-INT-001\*\*: The system shall provide a RESTful API for integration with third-party identity verification services (e.g., Auth0, Firebase Authentication).   
 \*Priority: Must Have\*   
 \*Rationale: Ensures secure and scalable authentication and verification capabilities.\*   
 \*Source: SRL-5.1\*   
 \*Acceptance Criteria: The system must support secure API calls and return standardized error codes and success responses.\*  
  
- \*\*C-INT-002\*\*: The system shall provide a RESTful API for integration with payment gateways (e.g., Stripe, PayPal).   
 \*Priority: Must Have\*   
 \*Rationale: Ensures seamless and secure payment processing and dispute resolution.\*   
 \*Source: SRL-5.1\*   
 \*Acceptance Criteria: The system must support secure API calls to each specified payment gateway and return standardized transaction and dispute statuses.\*  
  
- \*\*C-INT-003\*\*: The system shall support exporting data in CSV and PDF formats, with encryption for data sent over the network or stored in user-accessible files.   
 \*Priority: Should Have\*   
 \*Rationale: Provides flexibility for data usage and sharing while maintaining data security.\*   
 \*Source: SRL-5.4\*   
 \*Acceptance Criteria: Exported files must be encrypted using AES-256 or equivalent when shared or stored.\*  
  
## 5.4 Design and Implementation Constraints  
  
- \*\*C-DIS-001\*\*: The system shall implement role-based access control (RBAC) to manage access to sensitive actions and data.   
 \*Priority: Must Have\*   
 \*Rationale: Ensures that only authorized users can perform actions based on their roles (e.g., customer, admin).\*   
 \*Source: SRL-5.3\*   
 \*Acceptance Criteria: Access control policies must be enforced at both the UI and backend API levels.\*  
  
- \*\*C-DIS-002\*\*: The system shall maintain an audit log of all sensitive actions, such as dispute initiation, payment method deletion, or access to payment history.   
 \*Priority: Must Have\*   
 \*Rationale: Provides traceability and accountability for all high-risk operations.\*   
 \*Source: SRL-5.3\*   
 \*Acceptance Criteria: Audit logs must be timestamped, include the user ID, and be retained for at least 12 months.\*  
  
- \*\*C-DIS-003\*\*: The system shall not require external communication during the dispute resolution process.   
 \*Priority: Should Have\*   
 \*Rationale: Reduces dependency on external systems and ensures a self-contained dispute workflow.\*   
 \*Source: SRL-7\*   
 \*Acceptance Criteria: The dispute resolution process shall operate entirely within the system without requiring external service calls or user input from outside the platform.\*  
  
- \*\*C-DIS-004\*\*: The system shall implement adaptive re-authentication for sensitive actions, which may be skipped on trusted devices.   
 \*Priority: Should Have\*   
 \*Rationale: Balances security and user experience by reducing unnecessary friction on known devices.\*   
 \*Source: FR-20\*   
 \*Acceptance Criteria: Re-authentication prompts shall be skipped on devices marked as trusted by the system, with a clear UI indication that the action is allowed.\*  
  
- \*\*C-DIS-005\*\*: The system shall not allow the use of deprecated or insecure cryptographic algorithms (e.g., MD5, SHA-1).   
 \*Priority: Must Have\*   
 \*Rationale: Ensures data confidentiality and integrity using modern cryptographic standards.\*   
 \*Source: NFR-3\*   
 \*Acceptance Criteria: All cryptographic operations must use algorithms such as AES-256 and SHA-256 or higher.\*  
  
## 5.5 Other Constraints  
  
- \*\*C-OTH-001\*\*: The dispute resolution process shall be self-contained and must not require users to navigate to external websites or services.   
 \*Priority: Should Have\*   
 \*Rationale: Ensures a consistent and secure user experience throughout the platform.\*   
 \*Source: SRL-7\*   
 \*Acceptance Criteria: All dispute-related actions must be initiated and completed within the GAMMA-J Web Store interface.\*  
  
- \*\*C-OTH-002\*\*: The system shall not allow the use of unencrypted HTTP for any communication between client and server.   
 \*Priority: Must Have\*   
 \*Rationale: Ensures that all data is protected from interception and tampering during transit.\*   
 \*Source: SRL-5.2\*   
 \*Acceptance Criteria: All network communications must be encrypted using TLS 1.3 or higher.\*  
  
- \*\*C-OTH-003\*\*: The system shall not store or process user financial data on any system outside the scope of its secure backend infrastructure.   
 \*Priority: Must Have\*   
 \*Rationale: Minimizes the risk of data exposure to third-party systems not under direct control.\*   
 \*Source: NFR-2\*   
 \*Acceptance Criteria: All financial data shall be processed and stored within the system’s secure, internal database environment.\*  
  
- \*\*C-OTH-004\*\*: The system shall not permit the use of third-party libraries that are not actively maintained or have known vulnerabilities.   
 \*Priority: Should Have\*   
 \*Rationale: Ensures that all software dependencies are secure and up-to-date.\*   
 \*Source: NFR-1\*   
 \*Acceptance Criteria: All third-party libraries used in the system must be validated against a known vulnerability database and have active support.\*