## 1. Introduction

### 1.1 Purpose

The purpose of this document is to specify the functional and non-functional requirements of the ParaBank online banking website. It will serve as the basis for design, development, testing, and acceptance of the system.

### 1.2 Scope

The website allows customers to perform banking operations online via a web user interface, including login, registration, account management, transfers, bill payments, deposits/withdrawals, view history, etc. It also provides informational pages (About Us, Services, Locations, Contact Us) for public visitors.

### 1.3 Definitions, Acronyms, Abbreviations

* User / Customer = someone who has or wants a bank account and uses the website.
* Admin = internal bank staff who manage user accounts and system.
* ATM Services = online equivalents for withdraw/transfer/check balances/make deposits.
* Bill Pay = paying third-party bills via the system.
* Session = logged in period of user.

### 1.4 References

* The live site landing page and navigation structure. (see homepage)
* Applicable standards (web security, usability guidelines, banking regulations).

### 1.5 Overview

The remainder of this document details user-roles, overall system description, specific functional requirements, non-functional requirements (performance, usability, security, etc.), constraints, assumptions, and acceptance criteria.

## 2. Overall Description

### 2.1 Product Perspective

The website is a web-based banking portal integrated with the bank’s back-end systems (account database, transaction processing, billers interface). It is a replacement or enhancement of existing online banking portals.

### 2.2 Product Functions

High-level functions include:

* Customer registration & profile management
* Secure login/log-out
* Viewing account balances and history
* Transferring funds (internal/external)
* Deposits and withdrawals (via online interface)
* Bill payment module
* Informational pages: About Us, Services, Products, Locations, Contact Us
* Forgot login information recovery
* Admin interface (for bank staff)

### 2.3 User Classes and Characteristics

* **Customer (Registered user)**: has login credentials, uses full set of banking features.
* **Guest (Public visitor)**: can browse informational pages, register for account, but cannot access secured banking operations.
* **Administrator/Bank Staff**: manage users/accounts, monitor transactions, manage system settings.

### 2.4 Operating Environment

* Web browser support (modern browsers: Chrome, Firefox, Edge, Safari)
* Responsive design (desktop, tablet, mobile)
* Server environment: web server + application server + database server (details to be defined).

### 2.5 Design & Implementation Constraints

* Must comply with banking security regulations (e.g., encryption, authentication, transaction logging).
* Data privacy and GDPR/other regional compliance.
* Performance requirements: pages should load within an acceptable time.
* Availability requirement: system should be available 24×7 with scheduled maintenance windows.

### 2.6 User Documentation & Help

* Online help or FAQ section (e.g., “Forgot login info?”)
* Contact Us page with support details.

### 2.7 Assumptions & Dependencies

* Assumes reliable internet connectivity for users.
* Dependence on back-end banking systems being up and stable.
* Third-party biller networks are available and integrated.
* Assumes user has valid banking credentials after registration.

## 3. Functional Requirements

Below are the major functional requirements grouped by feature. Each requirement is given a unique ID for traceability.

### 3.1 User Registration & Authentication

* Req ID FR-1: The system shall allow a visitor (guest) to register a new account by providing required information (e.g., username, password, personal details).
* Req ID FR-2: The system shall send a verification email (or SMS) to confirm the user’s identity before enabling full login.
* Req ID FR-3: The system shall allow a registered user to log in using a valid username and password.
* Req ID FR-4: The system shall support “Forgot login info?” process allowing users to recover username/password via secure method.
* Req ID FR-5: The system shall automatically log out a user after a period of inactivity (e.g., 15 minutes) for security.
* Req ID FR-6: The system shall allow the user to log out manually.

### 3.2 Account Management & Dashboard

* FR-7: After login, the user shall see a dashboard listing all their bank accounts (account number, type, current balance).
* FR-8: The system shall allow the user to view detailed account information (opening date, interest rate if applicable, transaction limit).
* FR-9: The system shall allow the user to view transaction history for each account (date, description, amount, balance after transaction).

### 3.3 Fund Transfer

* FR-10: The system shall allow the user to transfer funds between their own accounts within the bank.
* FR-11: The system shall allow the user to transfer funds to another customer’s account at the bank (internal transfer) by providing recipient account number and amount.
* FR-12: The system shall validate sufficient funds, valid account numbers, and enforce transfer limits.
* FR-13: The system shall display a confirmation screen before finalizing a transfer, and send a confirmation notification (email or on-screen) once complete.

### 3.4 Bill Payment

* FR-14: The system shall allow the user to add new bill payees (select from list or enter manually) with required details.
* FR-15: The system shall allow the user to pay a bill by selecting a payee, entering amount and date, and choosing which account funds will be drawn from.
* FR-16: The system shall display scheduled payments and past bill payments (status, date, amount).
* FR-17: The system shall allow the user to cancel a scheduled bill payment before processing cutoff time.

### 3.5 Deposits / Withdrawals (Online ATM-Services)

* FR-18: The system shall allow a user to **make deposits** into their accounts via an online interface (assuming integration with deposit system).
* FR-19: The system shall allow a user to **withdraw funds** (subject to bank’s online withdrawal facility via portal; may redirect to branch).
* FR-20: The system shall allow the user to check their current available balance before making a withdrawal.

### 3.6 Informational Pages

* FR-21: The system shall provide a public “Home” page with navigation to major sections (About Us, Services, Products, Locations, Contact Us).
* FR-22: The system shall provide an “About Us” page describing the bank, mission, vision.
* FR-23: The system shall provide a “Services” page listing key services offered.
* FR-24: The system shall provide a “Products” page listing banking products (loans, deposits etc).
* FR-25: The system shall provide a “Locations” page showing branch/ATM locations (with map or list).
* FR-26: The system shall provide a “Contact Us” page with contact form and other contact details.

### 3.7 Admin Functions (Bank Staff)

* FR-27: The system shall allow admin users to log in using a separate admin portal with strong authentication.
* FR-28: The system shall allow admin users to view user accounts, enable/disable user access, reset user passwords.
* FR-29: The system shall allow admin users to view transaction logs, reconcile transfers, approve or reject flagged transactions.
* FR-30: The system shall allow admin users to publish news items/announcements (as seen on homepage “Latest News”).

### 3.8 Notifications & Messaging

* FR-31: The system shall send email or SMS notifications for key events (login from new device, large transfer, bill payment) as per configuration.
* FR-32: The system shall display on-screen confirmations or error messages for all major user actions (registration success/failure, transfer success/failure, payment scheduled).

### 3.9 Security & Audit

* FR-33: The system shall maintain an audit log of all significant events (login attempts, transfers, bill payments, admin actions) with user ID, timestamp, action type.
* FR-34: The system shall enforce secure password rules (minimum length, complexity, expiry).
* FR-35: The system shall use HTTPS for all interactions and encrypt sensitive data at rest and in transit.

## 4. Non-Functional Requirements

### 4.1 Performance

* NFR-1: The system shall support up to (for example) 500 simultaneous logged-in users with response times under 2 seconds for dashboard load.
* NFR-2: Pages shall load (first meaningful paint) within 3 seconds on a typical broadband connection.

### 4.2 Usability

* NFR-3: The user interface shall be responsive and usable on desktop, tablet and mobile browsers.
* NFR-4: The system shall provide consistent navigation, clear labels, accessible forms (with error-highlighting).

### 4.3 Availability & Reliability

* NFR-5: The system shall have 99.9% uptime (excluding scheduled maintenance).
* NFR-6: The system shall support backup and recovery procedures to restore data within a defined RTO/RPO.

### 4.4 Security

* NFR-7: The system shall protect against common web vulnerabilities (SQL injection, XSS, CSRF).
* NFR-8: User sessions shall timeout after inactivity (see FR-5) and session tokens shall be invalidated at logout.
* NFR-9: Sensitive data (such as passwords, personal details, account numbers) shall be masked or hidden from view (unless explicitly revealed by user).

### 4.5 Scalability & Maintainability

* NFR-10: The system architecture shall allow horizontal scaling (adding servers) to handle increased load.
* NFR-11: The codebase shall be modular, use documented APIs and allow future expansion (e.g., mobile app, new services).

### 4.6 Compliance

* NFR-12: The system shall comply with relevant banking regulations (e.g., data protection laws, electronic payments guidelines).
* NFR-13: The system shall support audit and regulatory reporting requirements.

### 4.7 Localization

* NFR-14: The system shall support multiple languages (if required) and adapt date/time/currency formats per region.

### 4.8 Accessibility

* NFR‐15: The system shall conform to WCAG 2.1 Level AA accessibility guidelines (for users with disabilities).

## 5. External Interface Requirements

### 5.1 User Interfaces

* The website shall have a well-designed HTML/CSS/JavaScript front end.
* The login page shall include “Username”, “Password”, “Forgot login info?”, “Register” links (as seen on home page). [parabank.parasoft.com](https://parabank.parasoft.com/parabank/index.htm)
* Navigation header shall include links: Home, About Us, Services, Products, Locations, Forum, Site Map, Contact Us. [parabank.parasoft.com](https://parabank.parasoft.com/parabank/index.htm)
* Dashboard includes lists of accounts, balances, quick action links (transfer funds, bill pay, account history).

### 5.2 Hardware Interfaces

* The system will run on standard web server infrastructure; clients use standard hardware (PC, tablet, mobile).

### 5.3 Software Interfaces

* Interface to back-end banking systems (account database, transaction processing).
* Interface to third-party biller systems for bill payments.
* Interface to email/SMS gateway for notifications.

### 5.4 Communications Interfaces

* All communication between client browser and server shall be over HTTPS (TLS).
* API endpoints shall accept/return JSON for internal services.
* Real-time or near-real-time updates for transactions.

## 6. System Attributes

* **Security**: described under Non-Functional.
* **Reliability**: error-handling, fail-safe behaviour, redundancy.
* **Maintainability**: code documentation, modular architecture.
* **Portability**: web application should work across browsers/devices.
* **Performance**: described.
* **Supportability**: logging, monitoring, alerts for system admins.

## 7. Other Requirements

### 7.1 Data Migration / Conversion

* If replacing existing system, the system shall support data import of existing customer accounts, balances, history.

### 7.2 Backup and Recovery

* Regular backups (daily full, hourly incremental); disaster recovery plan.

### 7.3 Legal & Regulatory

* Data retention policy as per banking regulations (e.g., retain transaction logs for X years).

### 7.4 Internationalization

* If future rollout to multiple countries, currency conversion, multilingual support.

### 7.5 Audit & Logging

* Audit trails for user/admin actions; log retention policy; retrieval for audit.

## 8. Acceptance Criteria

* All major user flows (login, registration, transfer, bill pay) work end-to-end with zero critical errors.
* Security testing passes (penetration testing, vulnerability scan) with no high or critical issues.
* Performance testing with target concurrent users meets response-time criteria.
* Usability testing indicates acceptable satisfaction scores across devices.
* Compliance checklist (regulatory, accessibility) is satisfied.
* User documentation/help pages available and accurate.

## 9. Glossary

* **Biller**: entity to which a payment is made (utilities, telecom, etc).
* **Dashboard**: main landing page after login summarising user accounts.
* **Transaction**: any credit/debit movement in an account (transfer, deposit, withdrawal, bill pay).
* **Session Timeout**: automatic log-out after inactivity.