User Acceptance Testing Plan

NimbusPay — Payment Processing Platform

Release v2.4.0 | April 14–25, 2026

Document Control

Document ID:	NIM-UAT-2026-041	Version:	1.0
Author:	Elena Vasquez, QA Lead	Status:	Draft
Reviewed By:	Marcus Chen, Product Owner	Classification:	Internal
Approved By:	Priya Kapoor, VP Engineering	Total Pages:	6

1. Introduction & Objectives

This User Acceptance Testing (UAT) Plan defines the strategy, scope, and execution framework for validating NimbusPay v2.4 against business requirements. The objective is to ensure the release meets stakeholder expectations and is fit for production deployment.

Primary Objectives:

- Validate that all functional requirements defined in BRD-NIM-2026-03 are implemented correctly.
- Confirm end-to-end business workflows execute without failure under realistic conditions.
- Verify that non-functional requirements (performance, security, usability) meet acceptance thresholds.
- Obtain formal stakeholder sign-off before production release.

2. Scope

2.1 In Scope

- User authentication module with role-based access control (RBAC).
- Payment processing engine — credit card and ACH transactions.
- Transaction reporting dashboard with export capabilities.
- Integration with external fraud detection service (Vertex Shield API).
- Administrative user management and audit logging.

2.2 Out of Scope

- Mobile application (iOS/Android) — tested separately under NIM-UAT-MOB-2026.
- Hardware security module (HSM) certification — pending external audit.
- Legacy batch processing module — deprecated from v2.4.

3. Test Environment & Setup

Environment:	UAT Staging (`uat.nimbuspay.internal`)
Server:	Application Server: 4 vCPU, 16 GB RAM, Ubuntu 22.04 LTS
Database:	PostgreSQL 15.4 (anonymized production snapshot dated 2026-04-10)
Browser:	Chrome 124, Firefox 125, Edge 124, Safari 17.4
Test Data:	Synthetic merchant accounts with transaction history spanning 90 days
Tools:	Jira (test case management), Zephyr Scale (traceability), Postman (API validation)

4. Test Scenarios & Acceptance Criteria

TC-001: User Login & Multi-Factor Authentication

Priority: Critical **Assigned To:** Sarah Lin, UAT Tester

Precondition: Valid user credentials exist in the staging identity provider.

Test Steps

1. Navigate to `https://uat.nimbuspay.internal/login`.
2. Enter valid email and password; submit the login form.
3. Enter the 6-digit OTP received via authenticator app.
4. Verify redirection to the dashboard.
5. Attempt login with an expired OTP (30-second window exceeded).
6. Attempt login with invalid credentials three times consecutively.

- Successful login redirects to dashboard within 2 seconds.
- Expired OTP is rejected with message "Authentication code expired. Request a new code."
- After three failed attempts, the account is locked for 15 minutes and an alert is logged.
- All login events (success and failure) are recorded in the audit trail.

TC-002: Credit Card Payment Processing

Priority: Critical **Assigned To:** David Okonkwo, UAT Tester

Precondition: Merchant account `MER-8842` is active with a valid processor configuration.

Test Steps

1. Initiate a payment of $149.99 using Visa test card `4111 1111 1111 1111`.
2. Verify that the fraud detection callout to Vertex Shield completes successfully.
3. Confirm the transaction appears in the merchant dashboard with status "Settled."
4. Initiate a payment of $2,500.00 using Mastercard test card `5555 5555 5555 4444`.
5. Simulate a declined transaction by using card `4000 0000 0000 0002`.
6. Process a partial refund of $75.00 against the settled Visa transaction.

- Payment authorization completes within 3 seconds for transactions under $500.
- Fraud detection response is received and logged; high-risk transactions are flagged for manual review.
- Declined transactions display a clear reason code (e.g., "Insufficient funds," "Do not honor").
- Partial refund is processed within one business-day settlement window and reflected in the ledger.
- All payment events are recorded with a unique transaction reference ID.

TC-003: Transaction Report Generation & Export

Priority: High **Assigned To:** Sarah Lin, UAT Tester

Precondition: At least 50 transactions exist for merchant `MER-8842` in the current billing cycle.

Test Steps

1. Navigate to Reports → Transaction Summary.
2. Set date range from 2026-04-01 to 2026-04-14.
3. Apply filter: Payment Type = "Credit Card," Status = "Settled."
4. Click "Generate Report" and verify on-screen preview.
5. Export the report in PDF and CSV formats.
6. Schedule a recurring weekly report to be emailed to `finance@nimbuspay.internal`.

- Report preview renders within 5 seconds for datasets up to 1,000 records.
- PDF export preserves all columns, formatting, and totals.
- CSV export includes headers and is importable into Excel without manual correction.
- Scheduled report is delivered to the specified recipient at the configured interval.
- Report footer displays generation timestamp and data freshness indicator.

TC-004: User Role Management & Access Control

Priority: High **Assigned To:** David Okonkwo, UAT Tester

Precondition: Admin user `admin@nimbuspay.internal` is logged in with full privileges.

Test Steps

1. Navigate to Admin → User Management.
2. Create a new user with role "Finance Viewer" and assign to merchant `MER-8842`.
3. Log in as the new Finance Viewer and attempt to access the Payment Processing module.
4. From the admin account, modify the user role to "Finance Manager."
5. Log in as Finance Manager and attempt to process a refund.
6. Delete the test user and verify the audit log records the deletion event.

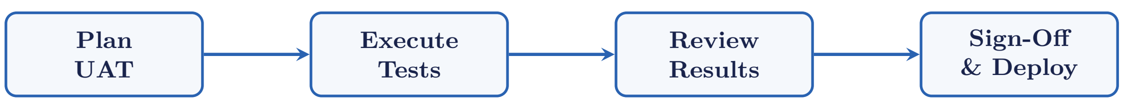
- Finance Viewer can access reports and dashboards but receives a 403 error when attempting payment operations.
- Finance Manager can process refunds up to $5,000 without additional approval.
- Role changes take effect immediately upon the next user session.
- User deletion cascades correctly: session tokens are invalidated and audit trail is preserved.
- All role modifications and access attempts are logged with timestamp and IP address.

5. Requirements Traceability Matrix

Req. ID	Requirement Description	Test Case	Status	Verified By
REQ-AUTH-01	User login with email/password and MFA	TC-001	✔ Pass	S. Lin
REQ-AUTH-02	Account lockout after three failed attempts	TC-001	✔ Pass	S. Lin
REQ-PAY-01	Credit card payment authorization	TC-002	✔ Pass	D. Okonkwo
REQ-PAY-02	Fraud detection service integration	TC-002	✔ Pass	D. Okonkwo
REQ-PAY-03	Declined transaction handling with reason codes	TC-002	✔ Pass	D. Okonkwo
REQ-PAY-04	Partial refund processing	TC-002	✔ Pass	D. Okonkwo
REQ-REP-01	Transaction report generation with filters	TC-003	✔ Pass	S. Lin
REQ-REP-02	PDF and CSV export functionality	TC-003	✔ Pass	S. Lin
REQ-REP-03	Scheduled report delivery via email	TC-003	🕒 Pending	S. Lin
REQ-RBAC-01	Role-based access control enforcement	TC-004	✔ Pass	D. Okonkwo
REQ-RBAC-02	User role modification with immediate effect	TC-004	✔ Pass	D. Okonkwo
REQ-RBAC-03	Audit logging of all access and role changes	TC-004	✔ Pass	D. Okonkwo

ℹ Note: REQ-REP-03 is pending email delivery infrastructure configuration by the DevOps team (ticket: OPS-1287).

6. UAT Process Flow



7. Sign-Off

By signing below, each stakeholder confirms that the UAT results meet the acceptance criteria and that NimbusPay v2.4 is approved for production release.

Role	Name	Signature	Date
QA Lead	Elena Vasquez		
Product Owner	Marcus Chen		
VP Engineering	Priya Kapoor		
Business Sponsor	Akira Tanaka		