

Flowpense – Product Requirements Document (PRD)

Document Control

Item	Detail
Version	0.2 (Consolidated MVP)
Date	09 Aug 2025
Author	Product Team – Daniel Ololo
Reviewers	Engineering Lead, Design Lead, Compliance Lead

Change Log

- v0.2: Renamed to Flowpense, added BVN/KYC, Hybrid card issuance (Named vs Department), Corporate Wallet model, Compliance flows, Backend architecture & data model, API specs, Super Admin portal, AI Policy Agent, Security & Ops.

1. Purpose

Flowpense is a corporate card & expense-management platform for Nigeria and Africa. It enables organisations to issue controlled payment cards (virtual/physical), automate approvals, capture receipts, and gain real-time visibility into spend — Africa-first, CBN-compliant, and BVN-aware.

2. Scope

In scope (MVP)

- **Company Admin Portal (finance ops)**
- **Employee Web & Mobile (PWA is fine for v1)**
- **Card request & issuance via issuer/BaaS partner**
- **Corporate Wallet (shared pool)**
- **Hybrid card model (Named Card w/ employee BVN; Department Card using company BVN on file)**
- **KYC/BVN capture & verification**
- **Spend policies, multi-level approvals, receipt OCR**
- **Integrations hub (CSV + basic QuickBooks/Xero export)**
- **Analytics & reporting**
- **Super Admin portal (platform-level)**

Out of scope (MVP)

- **Full public marketing site (separate project)**
- **In-app cross-border FX cards (plan Phase II)**
- **Credit/overdraft lines (Phase III)**

3. Glossary

- **BVN: Bank Verification Number (Nigeria)**
- **KYC: Know Your Customer (entity + person)**

- **MCC: Merchant Category Code**
 - **BaaS: Banking-as-a-Service/Issuer processor**
 - **Named Card: Card issued to an employee (individual BVN)**
 - **Department Card: Card issued under company BVN; assigned custodian**
-

4. Personas & Roles

Persona	Key Goals	Primary Interface
Org Admin / Finance Lead	Control spend, ensure compliance, reconcile books	Admin Portal
Team Leader / Approver	Approve or reject team expenses, monitor budgets	Admin Portal
Employee Card Holder	Pay for work expenses, submit receipts	Employee App (Web/PWA)
Flowpense Super Admin	Platform health, billing, compliance oversight	Super Admin Portal

5. Compliance (Nigeria, Expansion-Ready)

5.1 CBN & BVN Model (Nigeria)

- Every account or card must link to a BVN.
- Hybrid issuance:

- **Named Card (Employee):** Employee BVN + KYC required; card shows employee's name; draws from Corporate Wallet.
- **Department Card (Shared):** Uses Company KYC vault + Admin BVN on file; assign a custodian; still draws from Corporate Wallet.
- **Ledger & audit:** Full audit trail for KYC, approvals, spend and card lifecycle.
- **Sanctions/PEP screening:** via KYC provider if available (flag only in MVP, block in Phase II).

5.2 Company KYC (Entity)

- CAC Certificate, TIN/VAT, Registered Address (utility bill), Board Resolution/Mandate, 3-month bank statement, Admin BVN, Director IDs.

5.3 Individual KYC (Named Card)

- BVN, NIN/International Passport, Address proof, Selfie (liveness).

5.4 Regional Expansion Controls (SSA)

- Mirror local registrar docs; replace BVN with national ID equivalents; store normalized KYC schema.

5.5 Data Retention & Audit

- KYC artifacts retained 7 years minimum.
- Tamper-evident logs; immutable event store for compliance review.

6. End-to-End Admin Experience

6.1 Onboarding Journey

-
1. Email sign-up & 2FA
 2. Guided setup: Company Profile → Business Verification (KYC upload) → Funding Source (bank account) → Invite Team (roles) → Spend Policy (defaults)
 3. Compliance review → Status: Approved → Live.

6.2 Required Documents (Nigeria vs Other SSA)

Category	Nigeria	Other SSA
Incorporation	CAC (CAC1.1)	Registrar equivalent
Directors' IDs	NIN/BVN/Passport	Govt photo ID
Tax	TIN/VAT	Tax ID
Mandate	If signer ≠ Director	Same
Address	Utility bill (<3 mo)	Same
Bank Statement	3 months	Same

6.3 Admin Dashboard (Overview)

- KPIs: Active Cards, Spend MTD, Pending Approvals, Policy Breaches, Wallet Balance.
- Quick Actions: Create Card, Fund Wallet, Invite User, Export.

6.4 Corporate Wallet (Shared Pool)

- One Wallet per Company (NGN for MVP).
- Funding: Top-up by Admin (bank transfer or simulated for MVP).
- Authorisations check Wallet balance at approval; settlements debit Wallet.
- Wallet ledger supports credit, authorisation hold, settlement, refund, reversal.
- Card balances are logical limits, not separate accounts.

6.5 Card Lifecycle

1. Create Card: Choose Named or Department, set limits, categories, approvers.
2. KYC/BVN: Named → employee BVN; Department → company KYC on file.
3. Issue: Provision via issuer API (PAN/token).
4. Freeze/Unfreeze: API call to issuer.
5. Terminate/Reassign: Cleanly close; return funds to Wallet; ensure balance zero before reassign.

6.6 Expense Management

- Real-time Feed (auth & settlement).
- Auto-Categorisation by MCC (+ rules override).
- Receipt OCR & matching.
- Approval Workflow:
 - < ₦10k → Auto-approve (if policy enabled)
 - ₦10k-₦50k → Team Leader

- **¥50k → Team Leader + Admin**
- **Exceptions Queue: Missing receipts, duplicates, declines.**
- **Export/Sync: CSV, QuickBooks/Xero (basic).**

6.7 Integrations Hub

- **Accounting: QuickBooks, Xero, Zoho (export + later API).**
- **Sheets: Google Sheets & Microsoft Excel Online (push).**
- **BI/Data: REST & Webhooks for Power BI/Looker/Tableau.**
- **OAuth/API keys, chart-of-accounts mapping, sync schedule.**

6.8 Analytics & Reporting

- **Dashboards: Spend vs Budget, Top Merchants, Category Heatmap, Policy Compliance %, Burn Rate.**
- **Builder: Pivot by Date/Dept/Card/Employee.**
- **Exports: PDF, CSV, JSON; scheduled email/SFTP.**

6.9 Settings

- **Profile, Roles & Permissions (granular), Spend Policies (limits, merchant rules), Notifications (Email/SMS/Slack/Push), Security (2FA, API tokens, IP allow-lists), Billing & Plans.**

7. Employee & Approver UX

7.1 Employee

- Accept invite → 2FA.
- Home: Remaining limit, quick receipt upload.
- Purchase: Push notification; attach receipt; add note; view status.
- Personal insights + policy reminders.

7.2 Team Leader / Approver

- Approvals inbox (filters).
 - Team budgets (allocated vs spent).
 - Real-time over-budget alerts.
-

8. Super Admin (Flowpense Platform)

- Overview: Companies, active users, wallet volume, requests (24h/7d/30d), AI policy adoption.
- Company Management: Search, view KYC status, limits, feature flags, suspend/activate, assign account manager.
- User Management: Risk flags, disable/reset, platform support reps.
- Wallet Monitoring: Aggregate inflow/outflow, suspicious top-ups.
- AI Policy Engine Panel: Adoption & effectiveness, override defaults, upload localisation prompts.
- Billing: Plan usage, invoices, failed payments, promos.

- Compliance/KYC: Status dashboards, document flags, lockout rules.
 - Ops/Logs: API health, audit logs, ticketing, backup/export.
-

9. Technical Architecture

9.1 System Overview

- Frontend: Next.js + Tailwind + shadcn/ui (Admin, Employee, Super Admin).
- Backend: Node.js (Express/Fastify) or NestJS for stronger module boundaries.
- DB: Postgres (primary), Redis (caching & queues).
- Storage: S3-compatible (KYC docs, receipts).
- Messaging/Queues: Kafka or lightweight BullMQ (MVP: BullMQ/Redis).
- Issuer/BaaS: Partner API for card lifecycle, auth/settle webhooks.
- KYC: SmileID/VerifyMe APIs; NIBSS BVN check via provider.
- OCR: Tesseract/Cloud OCR (MVP).
- Observability: Prometheus/Grafana (metrics), ELK/Opensearch (logs), Sentry (errors).
- Infra: Containerised (Docker), deploy to AWS/GCP; secrets in Vault/SSM; WAF + CDN.

9.2 Data Model (Key Tables)

- companies(id, name, rc_number, tin, country, kyc_status, wallet_balance, created_at, ...)

- `company_kyc(company_id, docs[], admin_bvn_hash, status, reviewer_id, timestamps)`
- `users(id, company_id, email, role, status, bvn_hash?, kyc_status, phone, address, ...)`
- `cards(id, company_id, user_id?, type: 'named'/'department', custodian_user_id?, limits_json, status, token_ref, last4, brand, ...)`
- `wallet_ledger(id, company_id, tx_type: credit/hold/settle/refund/reversal, amount, currency, card_id?, request_id?, external_ref, balance_after, created_at)`
- `spend_requests(id, company_id, user_id, card_id, amount, currency, category, description, status: pending/approved/declined, policy_snapshot_json, created_at)`
- `approvals(id, request_id, approver_user_id, stage: finance/admin, decision, notes, decided_at)`
- `receipts(id, request_id, file_url, ocr_json, matched_tx_id?, status)`
- `policies(id, company_id, auto_approve_below, per_txn_limit, daily_cap, weekly_cap, require_receipt_above, category_rules_json, ...)`
- `audit_log(id, actor_type, actor_id, action, entity_type, entity_id, metadata_json, created_at)`
- `billing_subscriptions(company_id, plan, status, next_invoice_at, ...)`

9.3 API Surface (MVP)

Auth & Company

- `POST /auth/signup | POST /auth/login | POST /companies`
- `GET /companies/:id | PATCH /companies/:id`

KYC/BVN

- **POST** /kyc/company (upload docs)
- **POST** /kyc/user (employee KYC)
- **POST** /kyc/bvn/verify (proxy to provider)

Wallet

- **POST** /wallet/topup (admin only; records credit)
- **GET** /wallet/ledger?company_id=...
- **Webhooks:** /webhooks/settlement (issuer) → settle/adjust ledger

Cards

- **POST** /cards (type: named/department)
- **PATCH** /cards/:id (freeze/unfreeze)
- **DELETE** /cards/:id (terminate)
- **GET** /cards?company_id=...

Spend Requests & Approvals

- **POST** /spend-requests
- **POST** /spend-requests/:id/approve (role-gated)
- **POST** /spend-requests/:id/decline
- **GET** /spend-requests?company_id=...&status=...

Receipts

- **POST** /receipts (file upload)

- `GET /receipts/:id`

Policies

- `GET /policies/:company_id`
- `PATCH /policies/:company_id`

Analytics/Export

- `GET /reports/summary?company_id=...`
- `POST /exports/csv` (async job → downloadable link)

Super Admin

- `GET /admin/companies` | `PATCH /admin/companies/:id` (flags/limits)
- `GET /admin/metrics` | `GET /admin/audit`
- `POST /admin/feature-flags` | `POST /admin/billing/adjust`

All endpoints require JWT + role scopes; sensitive routes require IP allow-list or mTLS (Super Admin).

9.4 Eventing & Webhooks

- Inbound: Issuer auth/settlement events, KYC callbacks.
- Outbound: Company webhooks for approved spend, policy breach, month-end close.
- Event schema: `event_id`, `type`, `occurred_at`, `actor`, `entity`, `payload`.

9.5 Policy Engine (MVP)

- Rules: auto-approve threshold, per-txn limit, daily/weekly caps, category allow/deny, require receipt above X.
- Evaluates on request, auth, receipt upload; emits policy events.

9.6 AI Policy Agent (Advisory)

- Inputs: historical spend, approval latency, breach frequency, department mix.
 - Outputs: recommended thresholds (auto-approve, per-txn, daily), receipt rules, anomaly flags.
 - Delivery: Shows in Admin → “Apply” or “Dismiss” (record acceptance rate).
-

10. Multiple Cards, One Wallet – Rules

- All cards draw from Corporate Wallet (no sub-wallets in MVP).
 - Limits live on card/policy, not wallet partitions.
 - Authorisation checks: (1) Wallet available \geq amount, (2) Card per-txn limit, (3) Category rule, (4) Daily/weekly caps, (5) Policy exceptions.
 - Settlement debits wallet; reversal/refund credits wallet.
 - Department Cards must have custodian (user) for accountability and notifications.
-

11. Security, Risk & Compliance

11.1 Security

- TLS 1.3 in transit; AES-256 at rest; KMS/HSM-managed keys.
- Secret management via SSM/Vault; least privilege IAM; database row-level security by company_id.
- 2FA for Admin/Super Admin; IP allow-list for Super Admin.
- Regular pen-tests; dependency scanning.

11.2 Compliance

- PCI DSS v4 scope reduced by never storing PANs (use tokens).
- NDPR/GDPR data handling and DSR processes.
- Data residency: host regional mirrors as needed.
- Audit logs immutable and exportable.

11.3 Fraud & Abuse Controls

- Velocity rules (X txns in 3 hrs), MCC risk list, geo/IP anomalies.
- Freeze on repeated policy breach.
- Manual review queue (Super Admin).

11.4 BCP/DR

- Daily snapshots; PITR for Postgres; multi-AZ.
 - RTO \leq 2h, RPO \leq 15m (MVP target).
 - Incident runbooks; status page.
-



12. Non-Functional Requirements

- Availability: 99.9% monthly.
 - Performance: p95 API latency < 300 ms.
 - Scalability: Multi-tenant by company_id; sharding strategy vLater.
 - Observability: Metrics, tracing, structured logs, alerting on SLO breaches.
-

13. Pricing & Plans (MVP placeholder)

- Starter: ~~₦~~0/month — up to 3 users, basic approvals, CSV export.
 - Growth: ~~₦~~15k/month — up to 10 users, AI suggestions, integrations.
 - Enterprise: Custom — unlimited users, SSO, advanced analytics, priority support.
 - Transaction/issuer fees pass-through (per contract).
-

14. UX Deliverables

- Admin screens for: Choose Card Type, Named Card BVN/KYC, Department Card KYC, Wallet Top-Up, Approvals, Exceptions, Analytics.
 - Employee screens: Home, Spend Request, Receipt Upload, Status.
 - Super Admin: Overview, Companies, KYC, Billing, AI, Logs.
-

15. Rollout & Open Questions

Pilot: 3–5 companies (logistics, construction, NGO).

Bank/BaaS: Finalize with partner (card brand, BINs, webhook formats).

Open Questions

1. Which BVN provider SLA (latency/cost) for scale?
 2. Card network choice (Verve vs multi-brand) for widest acceptance?
 3. Do we support “per-project” tagging in MVP or Phase II?
-

16. Acceptance Criteria (MVP Exit)

- Company onboarded, KYC Approved, Wallet funded.
- Issue Named Card (employee BVN verified) and Department Card (company KYC).
- Perform authorisation → settlement → ledger updated → receipt matched → approvals recorded → export to CSV.
- Super Admin can view company, flags, suspend/reactivate, and see audit logs.