RaftWorks formerly LowCodeFlow

FREE RESOURCE

THE BUILD SHEET SERIES · 01

The Fintech MVP Launch Checklist

The **30 checks we run before any product that moves money goes live** — from compliance scoping to payment architecture to the launch-day QA that catches the expensive mistakes. Work through it top to bottom; every unchecked box is a conversation to have before launch, not after.

(01) Compliance scoping — before you build

1–2 days, saves months

- [ ] **Name the regulated activity.** Moving money, holding balances, lending, or just displaying data? Each has a different bar.
- [ ] **Ride on licensed rails where possible.** Stripe, Plaid, or a BaaS partner carries the license so your MVP doesn't need one.
- [ ] **Decide your KYC/AML story.** Use the processor's built-in KYC (e.g. Stripe Identity / Connect onboarding) instead of building your own.
- [ ] **Keep card data out of your stack entirely** — hosted checkout or tokenized fields keep you out of serious PCI scope.
- [ ] **Check data-residency rules** for your launch market (US vs UK/EU vs AU differ on where financial data may live).
- [ ] **Red flag:** any plan that involves holding customer funds in your own account "just for the MVP."

(02) Payments architecture

the core of the build

- [ ] **One source of truth for money movement:** an append-only transactions table — never editable rows.
- [ ] **Design for the unhappy paths first:** failed payments, partial refunds, disputes, and double-clicks.
- [ ] **Idempotency keys on every payment call** so retries can't charge twice.
- [ ] **Webhooks are the truth, not your UI.** Confirm state from processor webhooks, and handle out-of-order delivery.
- [ ] **Marketplace? Map the split flow on paper** (who pays fees, when payouts release, what happens on refund) before touching Stripe Connect.
- [ ] **Daily reconciliation report** — processor totals vs your ledger, from day one.

(03) Security & access

table stakes for trust

- [ ] **Role-based access** with the finance/admin role locked down separately from support staff.
- [ ] **Audit log every sensitive action** — who viewed, exported, refunded, or changed what, and when.
- [ ] **Encrypt sensitive fields at rest**, TLS everywhere, secrets in a manager (never in app code or no-code workflows).
- [ ] **Session timeouts + 2FA** on any account that can move money.
- [ ] **Least-privilege API keys:** restricted keys per integration, rotated on staff changes.

(04) Launch-day QA

the afternoon that saves you

- [ ] **Live penny test:** real card, small amount, full journey — charge, receipt, ledger entry, payout.
- [ ] **Force a failure:** declined card, expired card, abandoned checkout — confirm the user and the ledger both recover.
- [ ] **Full refund + partial refund** round-trip, including the emails they trigger.
- [ ] **Kill your webhook endpoint for 5 minutes** — confirm events replay and nothing is lost.
- [ ] **Check every money number renders correctly** in the two currencies/locales you launch with.
- [ ] **Ship with a rollback:** a documented way to pause new payments without taking the product down.

Not legal advice — confirm regulatory questions with counsel in your market