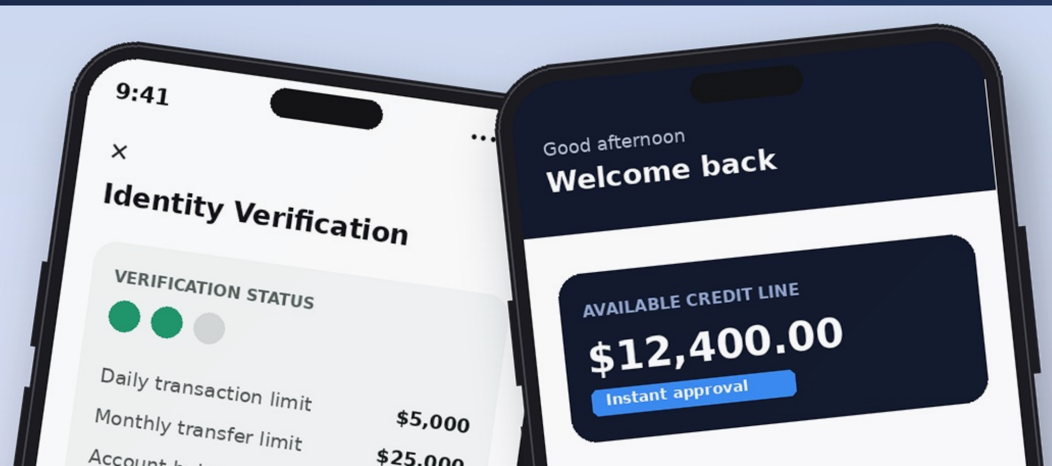
CASE STUDY · DIGITAL IDENTITY & COMPLIANCE

Building a Compliant KYC Experience for a Growing New Jersey Fintech

How a multi-layered identity verification framework helped a fast-growing consumer finance app scale onboarding across new U.S. states without compromising on regulatory compliance.

INDUSTRY	HEADQUARTERS	SERVICES
Consumer Fintech	**New Jersey, USA**	**Mobile & Backend Engineering**



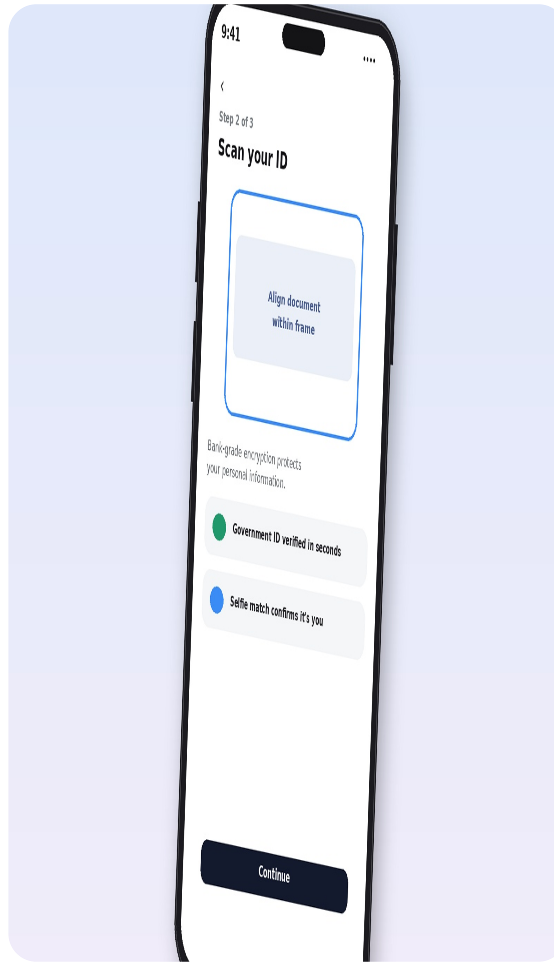
THE CLIENT

A digital-first lender built for the underbanked

Founded in the early 2010s and headquartered in New Jersey, the client set out to close the financial inclusion gap for underserved households and small businesses across the United States. Its mobile app gives customers a fast path to instant credit lines, everyday savings tools, and card products, all without the friction of a traditional bank branch.

Within a few years the platform had scaled to well over a million active customers, expanding state by state as demand grew. That growth brought a new kind of pressure: every new market came with its own identity-verification expectations, disclosure rules, and data-handling standards, and the product had to keep pace without slowing down the onboarding funnel that drove the business.

To manage that complexity, the client brought in an outside engineering partner to help redesign how identity verification worked across the platform, from the moment a user opens the app to the moment their account is fully active.



THE CHALLENGE

Compliance requirements were outrunning the product

As the user base crossed the million mark in under a year, the team's existing verification setup started to show its limits. What had worked for a single-market launch could not hold up under the weight of multi-state expansion.

- **Uneven data quality from verification vendors.** Different identity-verification providers returned inconsistent match confidence and formatting, making it hard to trust a single source of truth for a customer's identity.
- **Friction-heavy onboarding.** Mismatched records between government ID data, address history, and phone ownership were creating unnecessary manual review queues and abandoned sign-ups.
- **A patchwork of state-level rules.** Each new state came with its own requirements for identity proofing, disclosures, and recordkeeping, meaning a one-size-fits-all KYC flow was no longer viable.
- **Constantly shifting compliance standards.** Federal and state guidance around AML and consumer data protection kept evolving, requiring a verification stack that could be reconfigured quickly rather than rebuilt each time.

Rather than patch the existing system, the client's engineering leadership decided to rebuild the identity layer as a flexible, multi-provider framework that could absorb new regulatory requirements without a full redesign each time the company entered a new market.

THE PROJECT

A modular verification layer built for scale

The engineering team focused on three things at once: tightening the accuracy of identity checks, making the onboarding flow feel effortless, and building an architecture that could plug in new verification providers as new states came online.

Project goals

- Design a KYC framework flexible enough to satisfy legal requirements as the product expanded into new regions.
- Raise the bar on identity-verification accuracy to strengthen both compliance posture and customer trust.
- Cut time-to-launch in new markets by making it fast to onboard additional, localized verification providers.
- Keep onboarding fast and low-friction so verification improvements didn't cost the business new-user conversion.

What shipped

- A layered verification flow combining liveness-checked facial recognition with automated government ID document scanning.
- Cross-checks against Social Security number records, address history, and phone-number ownership to catch mismatches before they became compliance risk.
- An orchestration layer that could route a verification request to different identity-verification vendors depending on the customer's home state, so the company could onboard new regional providers without touching core app code.
- Direct integration with credit bureau and consent-management services to keep data-sharing disclosures aligned with state-level privacy requirements.

TECH STACK

Engineering choices built around flexibility and speed

The team standardized on a cross-platform mobile foundation paired with a modular backend, so verification logic could evolve independently from the release cycle of the app itself.

MOBILE

- React Native
- TypeScript
- Redux Toolkit
- Native Camera & Liveness SDKs

BACKEND & ORCHESTRATION

- Node.js (NestJS)
- GraphQL Gateway
- Event-driven microservices
- Kafka

IDENTITY & DATA

- PostgreSQL
- Redis
- Multi-vendor identity API orchestration
- Field-level encryption (AES-256)

INFRASTRUCTURE

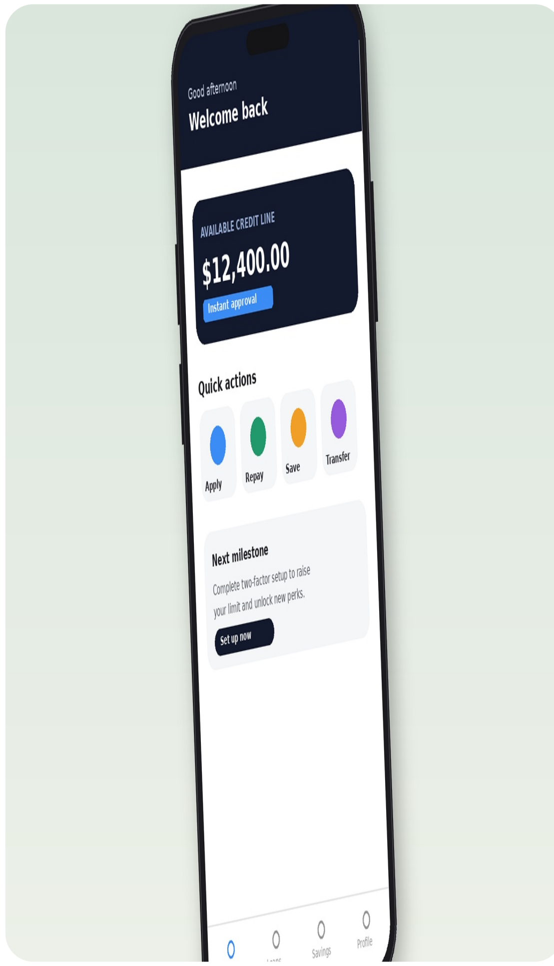
- AWS (ECS, Lambda, S3)
- Terraform
- Datadog monitoring
- CI/CD via GitHub Actions

This combination let the team ship a single, consistent onboarding experience across iOS and Android while keeping the identity-verification layer decoupled enough to swap or add vendors on a per-state basis, without a full app release.

THE RESULTS

Faster expansion, stronger compliance, happier users

The rebuilt KYC framework gave the company a verification system that could grow with the business instead of holding it back. New verification providers could be onboarded in weeks rather than quarters, and the improved matching logic meant fewer legitimate customers were caught in manual review.



< 6 weeks
Average time to stand up a new regional identity-verification provider

1M+
Active customers supported through the rebuilt onboarding flow

Multi-state
Compliant launches enabled without redesigning the core KYC flow

9/10
Client-reported satisfaction score for the engagement, reflecting both the pace of delivery and the durability of the resulting compliance framework.