CASE STUDY

EXTENDING IDENTITY GOVERNANCE TO DISCONNECTED APPLICATIONS WITH LIVE OAK BANK

In a regulated banking environment, identity work must be complete, accurate, & provable. Live Oak Bank leverages Opnova to automate identity & compliance workflows across disconnected & hard-to-integrate applications, reducing manual effort, lowering human-error risk, improving governance consistency, & creating capacity for higher-value governance work.

"Onboarding critical applications that lacked APIs to our identity program was one of our biggest challenges, & the alternatives we faced were limited."

Cassie Kenyon
Director of Identity & Access Management

Identity work that has to be provable

Live Oak Bank is the number one small business lender by dollar volume in the United States, operating as a federally regulated bank. Every joiner, mover, & leaver action, every entitlement change, & every access review must be complete, accurate, & produce documentation that a governing body can review on demand. The work is operational in execution & evidentiary in accountability.

Within Live Oak's application portfolio, a meaningful set of SOX-scoped & critical systems sat outside the reach of traditional identity governance tooling. Some exposed APIs, but bringing those applications into the bank's governance standard would have required significant platform-specific development for each application, plus ongoing maintenance liability. Lifecycle changes & access reviews on these systems were handled manually, with the same rigor as any governed process, just without the automation layer.

That approach was sustainable when the business was smaller. It became a constraint as the business grew. Delegating the work to business-unit administrators would have introduced inconsistency across SOX-scoped processes & fragmented existing controls. The team needed a way to govern these applications at the same cadence & high standards as the rest of the program, without scaling manual effort in lockstep with growth.

In a regulated environment, executing the action correctly carries a documentation requirement of equal weight. Each action must be reproducible on paper to internal audit, external auditors, & regulators. There is no margin for evidence that is partial, inconsistent, or hard to reconstruct after the fact.

Two categories of applications, one solution

Opnova fits two categories of applications that traditional identity governance tooling struggles with:

Critical applications that expose no integration surface, where the only access path is the same one a human operator uses

Critical applications that do expose APIs, where bringing them to the bank's governance standard would require significant platform-specific development per app, plus the ongoing maintenance burden that comes with custom code.

CASE STUDY

OPNOVA

The team's initial evaluation centered on two requirements that govern all identity work in regulated banking: accuracy & completeness.

Accuracy is the foundation. Automation in a regulated environment must produce the same result every time & produce it correctly. Live Oak validated repeatability in a pre-product environment first, against the specific applications & workflows where accuracy is most consequential, before bringing Opnova into live operations.

Completeness is the documentation standard. A lifecycle change must leave behind a record that is legible for audit, traceable end-to-end, & free of gaps in the chain of evidence. The team measured whether Opnova's documentation met the bank's standards without requiring additional reconciliation work.

Less manual work, more strategic capacity

With Opnova handling lifecycle & access work on the applications it covers, the operational profile of the IAM & service desk teams changed in three concrete ways.

Manual effort dropped sharply.

Provisioning, access requests, & entitlement changes for disconnected applications now execute quickly & consistently through Opnova, freeing capacity previously locked in transactional work.

Consistency improved time-sensitive work.

Joiner, mover, & leaver tasks now execute on cadence, keeping access changes aligned with when they should happen. That alignment supports stronger audit readiness.

Documentation became audit-grade by default.

Every action Opnova executes generates a record that meets the bank's evidence requirements, eliminating the secondary reconciliation work the team would otherwise perform.

Across all three, the team's attention has shifted toward work that compounds: governance design, controls maturity, identity architecture, & strategic projects that benefit from experienced human judgment.

> *"What makes Opnova such an asset to our team is not just the burden it replaced, but also its flexibility to scale to all of our different applications & processes."*
>
> **Chase Serif**
> Identity & Access Management,
> Information Security Associate

ABOUT OPNOVA

Opnova helps regulated organizations extend identity governance to applications that traditional IGA & ITSM platforms cannot reach: disconnected systems with no integration surface, & systems where API-based integration would require disproportionate custom development to bring under governance. The platform is built for the controls, documentation, & audit standards required in highly regulated industries, with a delivery model designed for the realities of bank IT environments.