Cover Page

State: Arizona

Agency: Arizona State Retirement System

Category: Cybersecurity

Project Title: Secure Site Identity Verification Project

Project Dates: 4/1/2025 – 5/21/2026

Contact: Trent Kendall, Chief Information Officer, trentk@azasrs.gov

Executive Summary

In early 2025, a surge in fraud activity across the U.S. pension sector hit our agency directly. While our secure member portal had held the line against earlier threats, increasingly sophisticated attacks made it clear that stronger protections were needed. We reprioritized our IT roadmap and launched the Secure Site Identity Verification Project — replacing knowledge-based authentication with multi-factor authentication and enhanced controls for high-risk member activities.

From conception to go-live, we completed market analysis, contract award, custom development, and full implementation in 13 months.

Securing What Members Earned: Modern Identity Verification for Public Pension Security

IDEA

The U.S. pension sector experienced a significant surge in fraud activity in early 2025, and our organization felt the impact. Bad actors had become adept at harvesting publicly available information to impersonate members and execute account takeovers. For a public pension fund managing $65 billion in member assets and serving 575,000 members and 3,000 employer accounts, the stakes could not be higher. A successful account takeover can result in the potentially irreversible misdirection of a member's retirement account.

Our previous secure member portal relied on usernames, passwords and knowledge-based authentication, methods increasingly vulnerable to sophisticated fraud. Incremental improvements would not be sufficient. We needed to fundamentally reimagine how we verify that the person creating or accessing a member account is actually that member.

The result was the Secure Site Identity Verification Project — a ground-up redesign of our portal's authentication and identity verification framework built on four pillars: multi-factor authentication, real-time government ID document verification, biometric liveness detection, and device risk assessment. Together, these controls close the gap that social engineering exploits.

This challenge is not unique to our state. Pension funds, benefits administrators, and government agencies across the country face the same threat landscape. Protecting constituent access to government services and the sensitive financial data behind it is directly aligned with the NASCIO State CIO Top Ten Priorities around cybersecurity and digital government. Any state agency managing sensitive constituent accounts online faces this same imperative.

IMPLEMENTATION

We approached this project with urgency balanced by diligence. Over three months, our team conducted structured market research including interviews, peer research and hands-on testing with all major identity verification vendors. We selected ID.me, the identity platform trusted by the IRS, the Social Security Administration, and dozens of other large-scale government and enterprise organizations. That pedigree mattered: it signaled proven scalability, regulatory alignment, and a support infrastructure capable of handling

constituent-facing complexity at our scale. Also a major factor was the dedicated ID.me end user support which meant that our call center could get out of the business of being a technical support team fielding lengthy calls walking people through a myriad of potential technical issues.

In July 2025, a dedicated internal development team was assigned full-time to the implementation. The project required a complete reimagining of the registration and login experience for both members and employers — not a patch on existing architecture, but a full replacement of the authentication layer. Credential management was migrated entirely from our pension administration system to ID.me, eliminating a significant attack surface. High-risk workflows — such as account refunds — were further hardened with identity verification checkpoints including liveness checks and document uploads.

Stakeholder alignment was maintained throughout. IT leadership, pension administration, member services, and employer-facing teams were engaged at each phase to ensure the solution met operational requirements without disrupting mandatory employer reporting functions. From conception to go-live, the entire project was completed in 13 months.

A brief overview of the technical architecture: our portal is a custom, self-managed application integrated with our pension administration system. ID.me was implemented as the authentication and identity layer via API integration, fully decoupling credential management from our core system and concentrating it in a purpose-built, federally trusted platform.

IMPACT

Before this project, our portal's security posture relied on credentials and knowledge-based authentication managed within our pension administration system — an approach that had become a liability against modern social engineering. Today, that vulnerability is closed, and $65 billion in member retirement assets is protected by the same identity infrastructure trusted by federal agencies.

The numbers tell the story:

- **265,000 member logins per year** are now authenticated through ID.me's multi-layered identity verification framework
- **3,000 employer accounts** transitioned to the new platform with zero disruption to mandatory reporting services. This implementation also eliminated employer account sharing which was a significant problem prior to ID.me

- **Site access and login-related call duration has dropped 15%** despite call volume holding steady, suggesting members are resolving issues faster with ID.me's dedicated support model. Historical call volume for these issues is 18,000 per year. Since going live we have seen the duration of these calls reduced by 15%. We expect the duration of these calls to continue to decrease.
- **Zero fraud incidents identified** in the five weeks since go-live. A promising early signal, though the team continues to monitor closely as the platform matures

The rollout achieved something rarely guaranteed in large-scale technology transitions: zero technical issues or bugs and zero disruption to member and employer services. While some members encountered friction during new registration, every issue was resolved through ID.me's customer support — and in each case, the root cause was user error, not a system problem. That track record reflects the professionalism and skills of our implementation team.

Authentication and credential management are now fully handled by ID.me, offering members a modern range of authentication options: username and password with MFA, passkeys, authenticator apps, hardware security keys, and single-use backup codes. Identity verification — including biometric liveness detection, government ID document upload and veracity check along with real-time device risk assessment — is embedded at both account setup and high-risk activity checkpoints.

Looking ahead, the platform will be maintained and kept current as ID.me continues to evolve — ensuring our security posture advances alongside the threat landscape without requiring additional large-scale implementation efforts. The initial investment has delivered a durable, enterprise-grade identity foundation that will protect our members' retirement security for years to come.