Securing Trust in Public Retirement Systems

Balancing Risk with Experience

LexisNexis®
RISK SOLUTIONS

Public retirement systems are a financial lifeline for millions of Americans, managing trillions of dollars in assets. These programs carry the dual responsibility of providing a **seamless, trustworthy experience and protecting funds from fraud** for beneficiaries accessing their accounts.

Retirees expect quick, intuitive access to their benefits without unnecessary friction. However, as fraud tactics evolve—with synthetic identities, automation, and account takeovers leading the way—systems that rely on outdated identity verification are increasingly vulnerable. The challenge is clear: **retirement systems must balance risk reduction with an improved customer journey.**

FACT:

The National Association of State Retirement Administrators (NASRA) reports that public pension funds collectively manage

over $5.6 trillion in assets.

NASRA Public Fund Survey

The Experience Imperative

Employee pension and retirement systems must **deliver modern, intuitive digital experiences** that inspire trust and reduce friction for legitimate beneficiaries.

Complex sign ins frustrate users. If access is slow or cumbersome, beneficiaries may abandon portals or flood call centers with support requests.

Trust is built on simplicity. Fast, seamless onboarding and account access can signal to retirees that the agency is modern, secure, and trustworthy.

Experience and security are not opposites. When implemented correctly, stronger fraud controls can make the user journey smoother by reducing unnecessary steps.

SURVEY INSIGHT:

74% **of U.S. respondents said they expect digital government services to be as good or better than private-sector digital services.**

BCG

The Evolving Threat Landscape

Fraud risks in retirement systems are not static. As technology advances, so do the methods fraudsters use to exploit weaknesses. Traditional processes, while once effective, are increasingly challenged by today's sophisticated schemes.

Synthetic Identity Fraud

Fraudsters can blend legitimate and fabricated data—such as Social Security numbers and dates of birth—to create synthetic "ghost" beneficiaries. These identities can pass basic verification checks and collect benefits for years undetected.

STATISTIC:

Losses from synthetic identity fraud crossed the $35 billion mark in 2023.

Federal Reserve Bank of Boston

Deceased Beneficiary Fraud

Delays in updating death records can allow benefits to continue flowing to deceased individuals. In some cases, family members or outside actors may intentionally conceal deaths to siphon funds.

EXAMPLE:

In FY 2024, 16 federal agencies reported nearly $162 billion in improper payments — more than $135 billion (≈ 84%) of which were overpayments, including payments to deceased individuals or those no longer eligible.

U.S. Government Accountability Office

Impersonation and Account Takeover

Fraudsters can use phishing, stolen credentials, or social engineering to gain access to legitimate beneficiary accounts. Once inside, they can redirect funds to accounts they control.

Insider Abuse

Employees or contractors with privileged access to beneficiary data can manipulate records, bypass controls, or even create fraudulent accounts. Without proper monitoring, insider risks can go unnoticed.

Automated and AI-Driven Attacks

Fraudsters now employ automation and AI-generated data to submit applications or probe identity verification systems at scale. These attacks overwhelm manual processes and exploit weaknesses in static defenses.

Balancing these demands requires agencies to rethink identity verification not as a barrier, but as an enabler of **trust, efficiency, and satisfaction**.

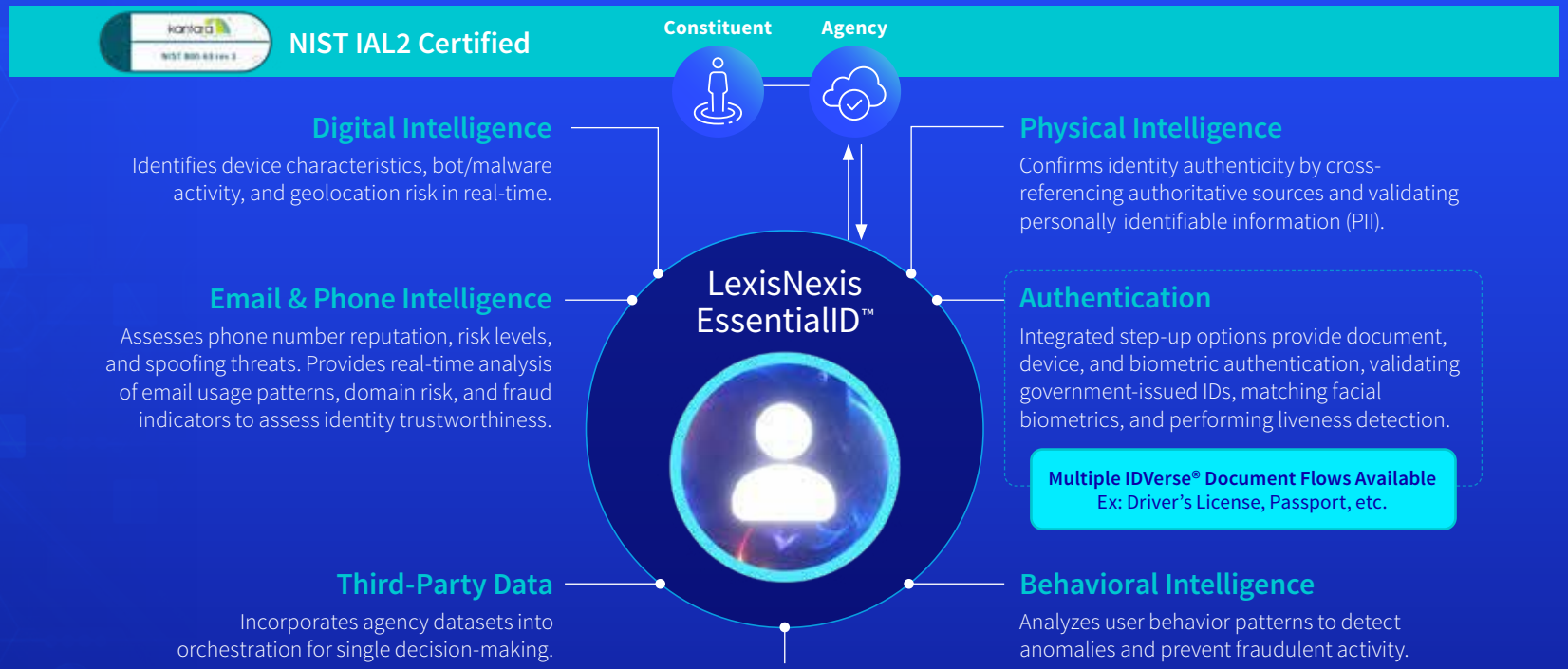
Modern Tools for a Trusted, Seamless Journey

The LexisNexis® Risk Solutions suite of tools can simultaneously protect against risk and deliver better experiences.

The solution is LexisNexis EssentialID™.

Delivered Via One Orchestration Platform

Built with Privacy, Flexibility, and Scalability in Mind



Experience Simple and Single Risk Decisioning: LexisNexis EssentialID™

Platform Orchestration
Award-winning solution delivered via a single API

Certified
NIST 800-63-3 IAL-2 Certification; NIST IAL-2 Certified

Simplified Usability
Fully hosted option at no additional cost

Transparent Results
Monitored and delivered by our LexisNexis® Risk Solutions Special Investigations Team

Early ROI
Easy to deploy for immediate results

1

Frictionless Onboarding

AI-powered digital identity verification confirms identities in seconds, helping to minimize drop-off and accelerating account access while spotting synthetic identities early.

Scenario: A new retiree applies online, and our solution confirms their identity using AI-driven checks, eliminating weeks of manual review.

2

Ongoing Trust

Behavioral biometrics analyze natural patterns—such as typing rhythm, mouse movement, and device use—to silently verify legitimate users. This process can flag account takeover attempts without requiring additional passwords or security questions.

Scenario: A retiree logs in from a new device, but their typing cadence and mouse usage confirm authenticity, so access is granted smoothly.

3

Continuous Verification

LexisNexis EssentialID provides ongoing checks against authoritative data sources, ensuring that only eligible, living beneficiaries receive benefits. This prevents improper payments and supports long-term program integrity.

Scenario: Our solutions detect that a beneficiary record doesn't match recent death registry updates, automatically flagging the account for review before funds are released.

LexisNexis EssentialID can form a **layered defense strategy** that strengthens security while improving the citizen experience.

CASE IN POINT:

LexisNexis Risk Solutions employs layered AI and consortium data to deliver near real-time identity proofing and continuous fraud monitoring, enabling agencies to shift from reactive to proactive risk management.

LexisNexis Risk Solutions

Roadmap for Agencies

Agencies don’t need to modernize overnight. A phased approach can allow systems to strengthen defenses and improve efficiency step by step.

Phase 1: Risk and Readiness Assessment

Evaluate current identity verification, monitoring, and fraud response processes. Identify gaps where fraud could slip through or where user friction is highest.

Phase 2: Pilot High-Impact Solutions

Start with initiatives that deliver immediate results, such as automated death record matching or synthetic identity screening.

Phase 3: Integrate Real-Time Verification

Adopt solutions to reduce manual workload, increase accuracy, and improve citizen experiences.

Phase 4: Continuous Monitoring and Improvement

Layer in behavioral biometrics and continuous eligibility checks to build long-term resilience. Monitor improvements using measures like:

- Reduction in improper payments
- Time saved on manual reviews
- Fraud detection vs. false positive rates
- Beneficiary satisfaction scores

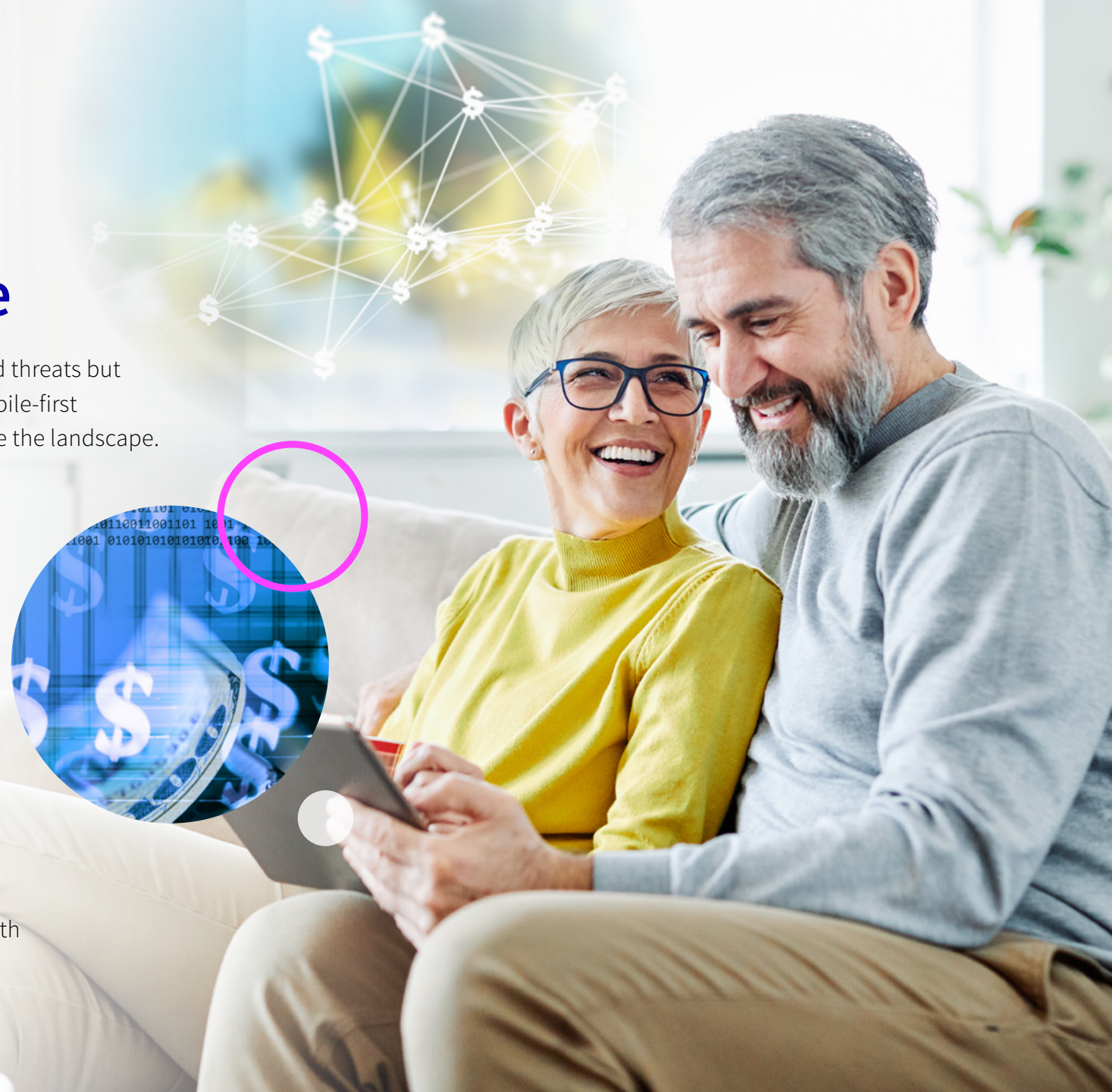
Looking Ahead: Building Confidence for the Future

Public retirement systems face increasing pressure—not only from fraud threats but also from rising citizen expectations. Emerging technologies like AI, mobile-first platforms, and cross-agency data collaboration will continue to reshape the landscape.

Agencies that modernize now will be better prepared to:

- **Detect and stop** synthetic fraud before benefits are paid.
- **Deliver seamless, secure access** to legitimate beneficiaries.
- **Preserve public trust** and program integrity in the face of growing scrutiny.

Fraud prevention is no longer just about protecting assets—it is about building **confidence, trust, and satisfaction** at every interaction. By balancing risk with experience, retirement systems can safeguard both **the funds they manage and the confidence of those they serve.**



Contact us today for more information.
Tel: 1-888-216-3544

LexisNexis®
RISK SOLUTIONS