LexisNexis®
RISK SOLUTIONS

ARTICLE

Understanding and Combating Fraud and Identity Risks in Public Sector Retirement Systems

Public sector retirement and pension systems face an increasing variety of fraud and identity-related risks. Scams targeting individuals aged 60 and older caused over $3.4 billion in losses in 2023—an increase of approximately 11% from the year prior. The average victim of elder fraud lost $33,915 due to these crimes in 2023.[1] Retirement systems must rise to the challenge, not only to protect their beneficiaries' financial security but also to maintain public trust in these essential programs.

This article will explore the primary challenges retirement systems face and the innovative solutions available to tackle fraud and identity risks effectively.

ARTICLE

The Challenges of Fraud in Public Sector Retirement Systems

Retirement systems, particularly in the public sector, are highly susceptible to fraud due to their complex structures and the sensitive nature of the information they manage. Key challenges include:

1. Digital Identity Fraud

With the digital transformation of retirement systems, cybercriminals have found new vulnerabilities to exploit. Techniques such as phishing, stolen credentials, and sophisticated fake documentation allow fraudsters to impersonate beneficiaries and divert payments.

2. Insider Threats

Insider fraud poses a significant threat to US retirement and employee pension systems. Internal threats account for approximately 20% of security threats across industries.[2]

3. Death Status Verification Gaps

Failure to accurately record death notifications can lead to fraudulent claims continuing for years. This lapse is a consistent target for criminals looking to extract funds unnoticed.

4. Cybersecurity Breaches

Hacking incidents and system compromises cause irreparable damage, leading to financial losses, compromised member data, and altered beneficiary records.

5. Financial Scams Targeted at Retirees

Elderly-specific scams, such as romance cons or government impersonation, often coerce retiree beneficiaries into sharing personal data, which fraudsters then exploit to siphon pension funds.

The Consequences of Fraud

The impact of fraud in retirement systems isn't just financial. Below are some of the broader consequences:

Depletion of fund reserves, threatening the long-term viability of pension systems

Emotional distress for beneficiaries, including shame and diminished trust

A lasting erosion of public confidence in the security of retirement systems

ARTICLE

Innovative Solutions to Fraud Prevention

To combat these escalating threats, retirement systems are turning to advanced technologies and proven strategies. Below are key measures being adopted to safeguard members and preserve public trust.

1. Advanced Identity Verification

Implement modern, AI-driven digital identity verification systems that cross-reference multiple data points to validate the authenticity of beneficiaries. Such systems analyze attributes like biometric data, behavioral patterns, and device fingerprints to ensure only legitimate claims are processed.

- **Real-time death status verification** helps pension systems flag beneficiaries who have passed away, closing common loopholes.
- **Predictive analytics significantly reduce false claims and increase auto-approval rates** for legitimate transactions.

2. Multi-Layered Cybersecurity Protocols

Enhanced cybersecurity measures can mitigate both external and internal threats. Examples include:

- **Two-factor authentication (2FA):** Provides an added security layer during account logins.
- **Dynamic risk-based authentication:** Adapts verification requirements based on suspicious behavior during digital transactions.
- **IP analysis and CAPTCHA tools:** Identifies and blocks coordinated fraud attempts.

3. Frequent Data Quality Checks

Proactively maintain clean, accurate, and enriched data records to prevent discrepancies.

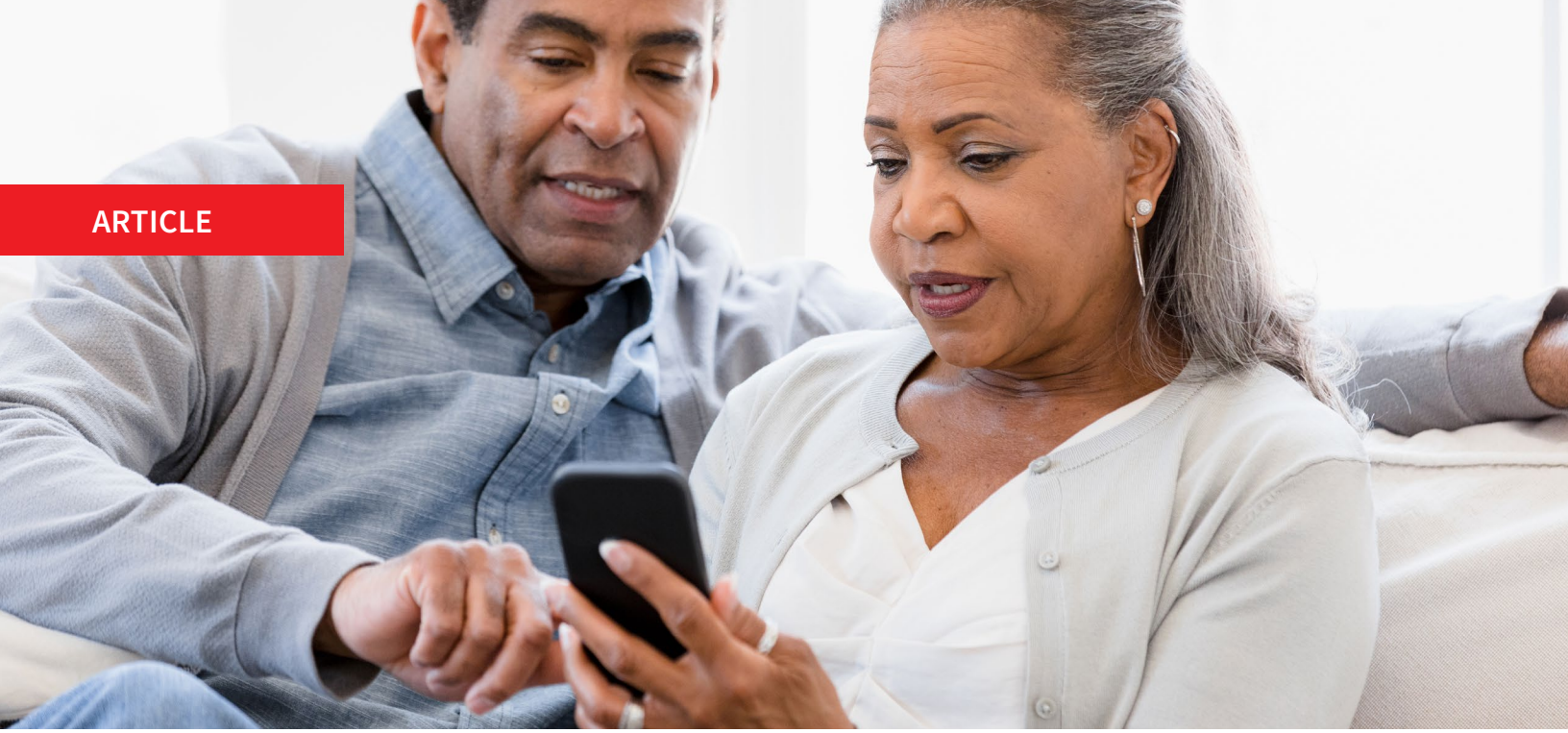
- **Validate member information by checking identity details**, death records, and bank account ownership using data cleansing techniques.
- **Store biometric and sensitive data using encrypted tokenization**, ensuring both accessibility and security.

4. Vigilance Against Insider Fraud

Combat insider threats with advanced access controls and monitoring solutions:

- **Limit employee privileges**, granting access only to data and tools essential to their specific roles.
- **Conduct regular audits** to identify anomalies in transactions or data manipulation.
- **Promote ethical practices within organizations** and establish a secure whistleblower system.

ARTICLE



5. Educating and Raising Awareness

Promote awareness and vigilance among members and administrators to prevent fraud attempts.

- **Engage retirees with targeted education campaigns** about scams and phishing threats.
- **Train staff to recognize red flags in transactions**, such as suspicious account changes or irregular payment requests.

6. Modernization and Automation of Legacy Systems

Outdated systems that rely heavily on manual processing are harder to safeguard. Modernized systems provide automated workflows, real-time oversight, and reduced human errors.

- **Implement robust, user-friendly self-service options** that still maintain high-security standards.
- **Utilize real-time fraud detection alerts** to quickly identify and neutralize emerging threats.

Case Study Insight

The Texas County & District Retirement System (TCDRS) effectively mitigated fraud risks by implementing advanced authentication tools, including **ThreatMetrix® for Government** for identity and device verification. This modernization allowed members to securely apply for benefits online and interact with the system confidently, achieving both efficiency and security. With layered measures like personalized security questions and real-time data validation, TCDRS significantly reduced fraud risks and elevated member satisfaction.

ARTICLE

Building a Fraud-Resilient Future

The challenges posed by fraud in retirement and public employee pension systems are steep, but they are not insurmountable. With strategic investments in technology, improved operational workflows, and early fraud detection solutions, agencies can significantly reduce costs, increase efficiencies while delivering better outcomes for beneficiaries and staff alike.

Key takeaways for retirement systems include:

- Modernize identity verification and minimize reliance on manual checks.
- Enhance cybersecurity protocols with multi-layered defenses and fraud detection.
- Foster collaboration with fraud prevention specialists and technology vendors for stronger defenses.

Looking to future-proof your retirement system against fraud risks? **Reach out to LexisNexis® Risk Solutions** for tailored solutions designed to support modernization, minimize risks, and optimize member experiences.

LexisNexis® RISK SOLUTIONS

https://risk.lexisnexis.com/government/retirement-systems
1-888-216-3544

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com, and www.relx.com.

1 https://www.fbi.gov/news/stories/elder-fraud-in-focus
2 https://www.plansponsor.com/insider-threats-are-disgruntled-employees-a-cybersecurity-risk/