LexisNexis®
RISK SOLUTIONS

2026 KEY RISK TRENDS ACROSS GOVERNMENT PROGRAMS

Identity is now the backbone of government service delivery. As fraud grows more sophisticated and digital channels expand, agencies must detect risk earlier—reshaping program risk in 2026.

DEPARTMENTS OF MOTOR VEHICLES (DMVs)

DMVs are facing growing identity risks as credentialing moves online. Fraudsters increasingly target license issuance systems to obtain state credentials using stolen, synthetic, or AI-altered identities—credentials that can then be used to access benefits or commit downstream fraud. Strengthening document authentication, liveness checks, and cross-agency data integration is becoming essential to protect the integrity of licensing ecosystems.

IDENTITY & CREDENTIALING RISK INDICATORS

Identity fraud cases continue to rise **12% annually**, signaling mounting pressure on ID-issuing authorities.[1]

Global identity fraud losses are projected to exceed **$50B in 2025**, increasing exposure for DMV-issued credentials.[2]

Florida recorded **528 identity-theft complaints and 2,163 fraud complaints per 100,000 residents,** indicating significant identity-system vulnerability.[3]

SOCIAL SECURITY ADMINISTRATION (SSA)

Although SSA's improper payment rates are low compared with many government programs, the scale of benefit disbursements means even small error rates can represent billions of taxpayer dollars. As digital access expands, SSA continues to face identity-driven risks tied to impersonation, account takeover, and benefit diversion.

SIGNALS OF EMERGING IDENTITY THREATS

Over **$1.5 trillion in annual SSA benefit disbursements**, meaning even low improper payment rates translate into billions of dollars in incorrect payments each year.[4]

Approximately **0.3% improper payments for Old-Age, Survivors, and Disability Insurance (OASDI) benefits and roughly 10% for Supplemental Security Income (SSI)**, driven primarily by overpayments related to eligibility and income reporting.[5]

Hundreds of millions of dollars in **annual consumer losses from government impersonation scams**, with SSA among the most frequently cited agencies targeted by fraudsters.[6]

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)

Medicaid and CMS can face substantial pressure from improper payments, provider fraud, identity misrepresentation, and duplicate enrollments across programs. Fraudsters can exploit complex eligibility rules and inconsistent data-sharing, while CMS works to strengthen analytics, cross-program verification, and provider screening to reduce systemic vulnerabilities.

PROGRAM INTEGRITY PRESSURES & RISK METRICS

CMS identified **2.8M individuals** enrolled in multiple Medicaid or ACA programs, with **$14B annually at risk**.[7]

Medicaid's improper payment rate reached **5.09% in 2024**, amounting to **$31.1B** in questionable payments.[8]

Medicaid Fraud Control Units reported **1,151 convictions** and **$1.37B in recoveries** in FY2024.[9]

LABOR & WORKFORCE AGENCIES

As unemployment insurance and workforce programs continue expanding digital access, identity-driven fraud remains a persistent integrity challenge. Fraud schemes increasingly involve stolen identities, falsified employment histories, and coordinated multi-state claims, placing sustained pressure on eligibility verification processes and payment accuracy.

UNEMPLOYMENT FRAUD PATTERNS TO WATCH

The U.S. Department of Labor reports unemployment insurance programs recorded an **improper payment rate of 14.41% in FY 2024**, reflecting ongoing eligibility and identity verification gaps.[10]

The Department of Labor Office of Inspector General reports that **stolen and misused identities remain a leading driver** of fraudulent UI claims, including cross-state filings and misrepresented employment histories.[11]

State and federal investigations continue to uncover **millions of dollars in fraudulent unemployment claims**, including organized schemes and public-sector cases, signaling ongoing exposure for workforce agencies.[12]

EDUCATION AGENCIES & INSTITUTIONS

Education systems can face vulnerabilities across financial aid, enrollment identity proofing, and payroll/credential fraud. As digital platforms expand, identity theft involving students, staff, and financial aid recipients is rising. Institutions are increasingly turning to stronger digital identity verification and analytics to protect funding and records.

IDENTITY & CREDENTIAL FRAUD TRENDS IN EDUCATION

Identity fraud is increasing approximately **12% annually**, affecting students, faculty, and financial aid processes.[13]

Fraudulent use of **stolen or fabricated identities to access federal student financial aid and enrollment benefits** has surged, with institutions reporting millions of dollars in lost financial aid and hundreds of thousands of suspicious applications.[14]

Colleges and federal authorities are increasingly identifying **"ghost student" and fake Free Application for Federal Student Aid (FAFSA) applications** leveraging stolen identities, prompting new identity verification requirements to curb financial aid fraud.[15]

SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM (SNAP)

SNAP faces rising fraud pressure as Electronic Benefit Transfer (EBT) theft, duplicate enrollments, and synthetic identities become more common. Fraudsters can exploit digital application workflows and gaps in identity verification. States are turning to analytics, orchestration, and cross-program matching to close vulnerabilities and improve benefit accuracy.

EVOLVING FRAUD & ELIGIBILITY RISK FACTORS

Fraudulent SNAP applications and post-issuance fraud **doubled from 2024 to 2025**, per LexisNexis® Risk Solutions.[16]

For every $1 in fraudulent SNAP benefits, agencies incur **$4.14 in total costs**.[17]

Identity fraud is accelerating across benefit programs.[18]

RETIREMENT & PENSION PROGRAMS

Retirement and pension systems can face targeted identity theft, improper benefit diversion, and fraudulent survivor claims. Although fraud incidence is lower than in some other sectors, each case can have substantial long-term financial impact. Strong identity proofing and ongoing authentication are increasingly essential for retirement and pension programs.

IDENTITY RISKS IMPACTING RETIREMENT BENEFITS

A Connecticut case resulted in **$370,000+ in fraudulently obtained** retirement and related benefits.[19]

Older adults increasingly report **$10,000+** losses to impersonation scams.[20]

Rising direct-deposit fraud has prompted targeted policy and program changes aimed at reducing improper payments and strengthening account verification controls.[21]

Building Resilient Public Services Through Better Identity Intelligence

In today's digital-first government, identity is the frontline of trust. As agencies accelerate modernization, every interaction becomes a moment of risk—or confidence. Citizens expect seamless access to essential services, while programs must be protected from increasingly sophisticated fraud and misuse.

LexisNexis® Risk Solutions empowers agencies to truly know who they serve—strengthening trust and securing access through authoritative data, advanced analytics, and trusted identity assurance. **The result: more resilient programs, stronger program integrity, and safer, smarter services for every community.**

LexisNexis®
RISK SOLUTIONS

For more information visit or call 1-888-216-3544.

[1] https://snappt.com/blog/identity-fraud-statistics/
[2] https://snappt.com/blog/identity-fraud-statistics/
[3] https://www.fox32chicago.com/news/states-most-vulnerable-identity-theft-fraud-2025-data
[4] https://www.ssa.gov/finance/2024/Full%20FY%202024%20AFR.pdf
[5] https://www.ssa.gov/finance/2024/Full%20FY%202024%20AFR.pdf
[6] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024
[7] https://www.cms.gov/newsroom/press-releases/cms-finds-28-million-americans-potentially-enrolled-two-or-more-medicaid/aca-exchange-plans
[8] https://ccf.georgetown.edu/2025/03/13/medicaid-fraud-the-improper-use-of-improper-payments/
[9] https://oig.hhs.gov/newsroom/videos/medicaid-fraud-control-units-annual-report-fiscal-year-2024/
[10] https://www.oig.dol.gov/public/DOL%202023%20Top%20Management%20and%20Performance%20Challenges.pdf
[11] https://www.oig.dol.gov/doloiguioversightwork.htm
[12] https://apnews.com/article/747b8018756ee36ded7a51869d9afa34
[13] https://snappt.com/blog/identity-fraud-statistics/
[14] https://www.proof.com/blog/ghost-students-stolen-identities-and-the-fafsa-fraud-crisis
[15] https://www.ed.gov/about/news/press-release/us-department-of-education-implement-new-identity-validation-processes-combat-student-aid-fraud
[16] https://risk.lexisnexis.com/about-us/press-room/press-release/20250923-tcof-snap
[17] https://risk.lexisnexis.com/about-us/press-room/press-release/20250923-tcof-snap
[18] https://snappt.com/blog/identity-fraud-statistics/
[19] https://www.ctinsider.com/news/article/hartford-ct-fraud-social-security-unemployment-20185543.php
[20] https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-data-show-more-four-fold-increase-reports-impersonation-scammers-stealing-tens-even-hundreds
[21] https://www.gao.gov/products/gao-23-106285