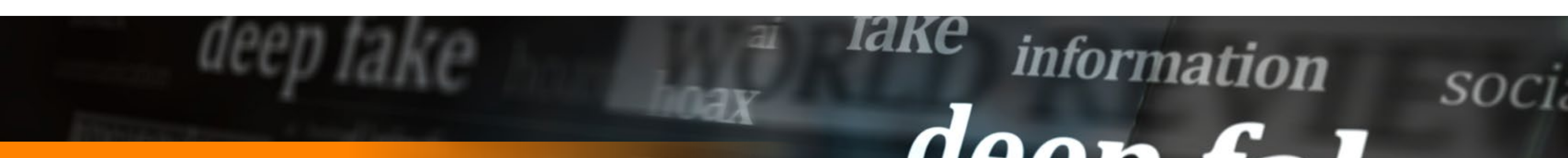
TOP 6 PUBLIC SECTOR FRAUD AND CYBER THREATS IN 2025

DISCOVER WHAT FEDERAL, STATE, AND LOCAL GOVERNMENTS MAY EXPECT FROM FRAUD AND CYBER THREATS THIS YEAR.

As we enter 2025, the fraud landscape continues to evolve rapidly, driven by technological advancements and increasingly sophisticated threat actors. Several key trends are emerging that government agencies should be aware of to protect themselves and those they serve.

Here are our predictions for the Top 6 Public Sector Fraud and Cyber Attack Threats – based on recent findings and statistics – that may escalate and proliferate throughout 2025.



1. Deepfake Media Fraud

Deepfake technology has become a significant concern in identity fraud – **one deepfake attempt now occurs every five minutes on average.** Criminals can create deepfake media – images, videos, or audio that depict real or non-existent people – by modifying an authentic source image or creating a synthetic one. They have also combined Generative Artificial Intelligence (GenAI) images with stolen personal identifiable information (PII) or entirely fake PII to create synthetic identities. The potential for deepfake media to be used in fraud schemes is one of several risks associated with emerging GenAI technologies that government agencies, institutions, and their customers may face.[1]

At the end of 2024, U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) **sounded the alarm in an alert**[2] about this growing and insidious threat. FinCEN has observed an increase in suspicious activity reporting by financial institutions describing the suspected use of deepfake media, particularly the use of fraudulent identity documents to circumvent identity verification and authentication methods.

2. Elder/Vulnerable Population Fraud

Fraud targeting vulnerable populations has been on the rise, leveraging sophisticated tactics like phishing, synthetic identity creation, and impersonation. **Older adults remain disproportionately affected**, with scammers targeting them through schemes designed to exploit their financial resources, trust, and sometimes their lack of familiarity with technology, such as:

- **FAKE LOTTERY WINNINGS**
- **INTERNAL REVENUE SERVICE (IRS) THREATS**
- **TECHNICAL SUPPORT CONS**
- **ROMANCE PLOYS**
- **MEDICARE/HEALTHCARE SCAMS**

These schemes, often perpetrated by individuals posing as government officials, family members, or legitimate companies, have a devastating impact. **Financial losses for those aged 60-69 are the highest among all age groups, with over $980 million stolen through fraud schemes.**[3] Yet, according to the National Adult Protective Services Association (NAPSA), only one in 44 cases of elder fraud is reported to authorities, meaning the vast majority of elder financial abuse goes unreported[4] – this is likely due to stigma and shame older adults may feel about being tricked. Educational initiatives and enhanced reporting mechanisms are crucial to combating this alarming trend and safeguarding the financial security and dignity of older populations.

Vulnerable groups, including low-income individuals and veterans,[5] also report increasing victimization through predatory scams, including imposter job offers and phishing attacks designed to extract sensitive information. Unfortunately, these populations can become targets due to limited access to fraud prevention resources and financial safety nets.

3. Unemployment Insurance Fraud

Unemployment insurance (UI) fraud continues to evolve, with perpetrators employing increasingly sophisticated methods – especially **identity theft via data breaches or phishing attacks to file fraudulent UI claims under stolen identities.** This approach not only diverts funds from legitimate claimants but also complicates detection, as the benefits are often directed to accounts controlled by the fraudsters. The U.S. Department of Labor has reported a significant number of fraud cases involving identity theft, underscoring the need for enhanced verification processes and public awareness to safeguard personal information.[6]

Another emerging scheme involves employers and **employees conspiring to report reduced hours or layoffs that haven't occurred,** enabling employees to collect UI benefits while still receiving full wages. This type of fraud exploits the trust-based nature of employer-reported data and can be challenging to detect without advanced analytics and cross-referencing of employment records. State departments of labor are increasingly leveraging advanced analytics to identify such fraudulent activities, aiming to protect the integrity of unemployment benefits programs.[7]

4. Supplemental Nutrition Assistance Program (SNAP) Fraud

The Supplemental Nutrition Assistance Program (SNAP) and other government benefits programs have faced increasing challenges in combating fraud. **In 2024, SNAP fraud continued to involve methods such as:**

- **IDENTITY THEFT**
- **ELECTRONIC BENEFITS TRANSFER (EBT) CARD SKIMMING**
- **SYNTHETIC IDENTITIES**

The **2024 LexisNexis® Risk Solutions True Cost of Fraud™ Study**[8] **indicated that agencies lose an average of $4.48 for every $1 in SNAP benefits fraud**, with electronic fraud accounting for a significant share. Additionally, the complexity of Integrated Eligibility Systems (IES), which link multiple welfare programs, has inadvertently created more vulnerabilities. Early-stage fraud detection strategies remain a challenge to government agencies, leading to delayed application processing and strained caseworker resources. Despite these issues, only 1–1.5% of SNAP benefits are typically confirmed as fraudulent, underscoring the program's rigorous safeguards and the need for more proactive fraud prevention measures at earlier stages.

Fraud investigations reveal that **states like California and New York**[9] **lead in the number of cases, while others, such as Massachusetts, report high average fraud amounts per disqualification**. These investigations commonly focus on anomalies in EBT transactions, such as excessive out-of-state spending or unusually high purchase amounts.Despite growing public skepticism, evidenced by only 47% of Americans trusting the SNAP program, these findings highlight the efficacy of its oversight mechanisms and the importance of continued investment in fraud detection technologies.[10]

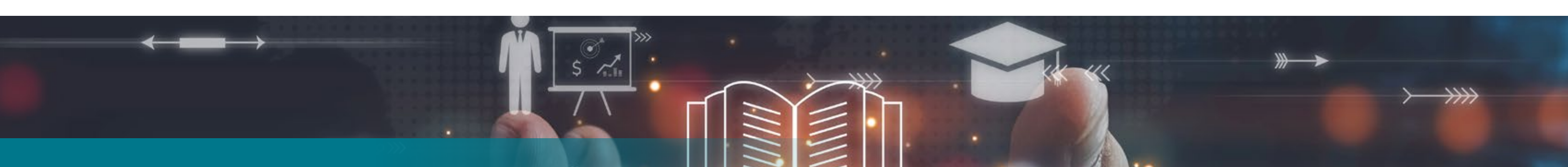
5. Department of Motor Vehicles (DMV) Fraud

The **target on Departments of Motor Vehicles (DMV) persists,** with fraudsters leveraging advanced technologies and exploiting the increasing digitization of government services – which include phishing attacks that deceive people into revealing personal information. The rise of GenAI has further complicated these threats, allowing fraudsters to produce convincing fake identities and documents, which enhances the credibility of their fraudulent schemes. Additionally, the proliferation of digital payment methods has opened other avenues for fraud, with criminals utilizing stolen credentials to execute illicit transactions.[11]

The impact of these fraud trends on citizens is profound, as they face increased risks of:

- **IDENTITY THEFT**
- **FINANCIAL LOSS**
- **ADMINISTRATIVE COMPLICATIONS**

Victims may experience **unauthorized transactions, compromised personal information, and the arduous process of rectifying the damage** caused by fraud attacks.



6. Higher Education Fraud

Higher education institutions are increasingly targeted by **new and sophisticated fraud schemes, notably using "ghost students" – fictitious enrollments created to exploit financial aid systems.** These schemes often involve the use of bots and fake accounts to automate the submission of fraudulent applications, making detection and prevention more challenging.[12]

Other unethical higher education fraud tactics include:

- **UNDERREPORTING INCOME AND ASSETS**
- **OVERSTATING THE NUMBER OF FAMILY MEMBERS IN COLLEGE**
- **SUBMITTING FALSIFIED TAX RETURNS**[13]

In California, community colleges have reported a significant rise in such fraud, with suspected bots representing 25% of college applicants as of January 2024. This surge has led to the **fraudulent disbursement of over $5 million in federal student aid to individuals** who enrolled in these colleges, received financial aid, and then disappeared.[14,15]

Higher education institutions are urged to **implement strict identity verification processes and utilize advanced technologies** to detect and prevent fraudulent activities. Additionally, **students should be vigilant against scams**, such as those involving unsolicited requests for personal information, which can lead to identity theft and financial loss.

A SOLUTION THAT WORKS

Secure access to government programs is essential for all citizens and **prioritizing a people-first approach while simultaneously preventing cyber threats is critical**. Identity isn't just a one-time transaction or event. It's ongoing, with a past, present, and future — constantly evolving. It is essential to have a comprehensive, long-term perspective on identity.

LexisNexis EssentialID™ is an award-winning, seamless, and secure identity orchestration platform providing multi-layered, fraud-resistant identity verification, third-party data integration and decision-making capabilities.

Balance Service and Trust

Generate more reliable and actionable outcomes through our 99.99% linking precision rate.

Protect your agency from risk by leveraging our adherence to strict ethical standards in data use and privacy and proven expertise in regulatory compliance.

Let us help protect your agency—starting today.

LexisNexis® RISK SOLUTIONS

Find out more about the power of LexisNexis EssentialID™. Scan the QR code or call us at 1.888.216.3544.

1. https://onfido.com/blog/top-fraud-trends-and-considerations-for-2025/
2. https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial
3. https://www.consumeraffairs.com/finance/identity-theft-statistics.html
4. https://www.napsa-now.org/additional-resources-for-financial-exploitation/
5. https://news.va.gov/135595/how-to-protect-yourself-from-cyber-attacks-and-scams/?utm_source=chatgpt.com
6. https://www.dol.gov/agencies/eta/UIIDtheft#:~:text=Unemployment%20Identity%20Fraud%20is%20on,was%20changed%20without%20their%20knowledge.
7. https://www.voyatek.com/insights/how-state-departments-of-labor-can-leverage-advanced-analytics-to-unemployment-insurance-fraud/
8. https://risk.lexisnexis.com/insights-resources/research/2024-true-cost-of-fraud-for-snap-and-ies-agencies
9. https://www.newsweek.com/snap-stolen-benefits-claims-skyrocket-1983882?utm_source=chatgpt.com
10. https://balancingeverything.com/welfare-fraud-statistics/
11. https://www.feedzai.com/blog/fraud-and-financial-crime-trends-to-watch-in-2024/
12. https://intelliboard.net/blog/ghost-students-and-financial-aid-fraud/
13. https://finaid.org/educators/fraud/
14. https://calmatters.org/education/higher-education/2024/04/financial-aid-fraud/
15. https://edworkforce.house.gov/news/documentsingle.aspx?DocumentID=410487

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 o¬ices 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.