AGENCY WATCH

5 FRAUD AND CYBER THREAT TRENDS IMPACTING PUBLIC SECTOR AGENCIES THIS YEAR

Government agencies know how challenging it is to stop criminal enterprises and cyber threats before they attack. Schemes are ever evolving and organized, as criminals constantly work to defraud agencies and access government funds using advanced digital and in-person schemes. **Here are the top 5 public sector focus areas and markets we believe will be particularly vulnerable to fraud and cyber threat escalation in 2024.**

1. Department of Motor Vehicles (DMV) Fraud

DMV scams are a form of phishing that take advantage of government offices' efforts to provide more services online, including driver's license renewal in many states. Crooks seek to lure motorists to phony versions of government websites on the pretext of helping them with tasks such as license renewal or title transfer. Data breaches have led to increases in fraud impacting DMVs.

Driver's licenses or other state identifications were exposed in 31% of breaches in the first half of 2023 (up from 14%) and exposure for checking or savings account numbers also doubled year over year.[1]

Spiking gas prices brought a new twist, according to the New York DMV: **Scammers are sending out texts claiming drivers are in line for a $1,500 fuel rebate from the state**, with a link to what looks like an authentic government site to enter personal information, which the crooks can use to commit identity theft.[2]

ID theft protection advocates say **criminal networks are focusing data breaches on DMVs** and organizations that have drivers' licenses, so they can **use license information to get government benefits and open bank accounts**.[3]

MITIGATION STRATEGY: Educate and remind drivers of the risks associated with identity theft. Implement a multi-layered solution approach using digital identity verification solution to protect drivers from identity theft.

2. Education/Student Loan Fraud

Student loans are a prime target for fraudsters seeking to abuse the system and obtain funds. Federal student loan fraud happens when a person, organization, or group falsifies information on a student loan application to illicitly obtain funds through the U.S. Department of Education.

Student loan payments restarted in October 2023 after a pause of more than three years – **fraudsters are trying to mislead borrowers** by offering to lower borrowers' monthly payments, avoid repayment or get their loans forgiven.[4]

The volume of **fraudulent texts spiked in August 2023** after the Biden administration announced its plan to forgive up to $20,000 in federal student loan debt per borrower. Before the announcement, RoboKiller was counting between 2 million and 3 million student loan scam texts per month – in August, that monthly total **rose to 9 million**.[5]

According to Forbes and anti-spam/scam platform RoboKiller, **Americans lost $5 billion to student loan fraud in 2022**. Borrowers received 700 million student-loan-related robocalls every month last year.[6]

MITIGATION STRATEGY: Assess and verify student identities before providing access to funding or student resources. Implement frictionless digital identity proofing capabilities to help verify and authenticate student identities without hindering experience expectations and service.

3. Social Security Fraud

Social Security imposter scams continue to be pervasive across the country, with scammers using targeted, sophisticated tactics to deceive people into providing sensitive, private information or money. Fraudsters will call, email, text, write, or send messages on social media claiming to be from the Social Security Administration, using Social Security-related images and jargon to appear as if they're associated with or endorsed by Social Security.

Social Security Numbers were exposed in 69% of breaches in 2023, up from 60% in 2022.[7]

More than $100 million is lost each year due to Social Security scams, new figures from the Federal Trade Commission (FTC) show. Already in 2023, the FTC has received reports of 164,413 government imposter scams, with social security scams being the most common of all.[8]

Between October 2022 and June 2023, **more than 55,000 people who answered calls from what they thought was the government agency said they were scammed**.[9]

MITIGATION STRATEGY: Awareness is key to minimizing fraud risk. Exercise caution whenever any person, business, or agency asks for a social security number. Agencies can consider adding additional protection layers for social security numbers and educate protection methods.

4. Supplemental Nutrition Assistance Program (SNAP) Fraud

SNAP services help people afford the nutritious food they need. Most SNAP benefits are used as intended — to supplement the food budgets of eligible families — but unfortunately, the program experiences fraud.

Every $1 value of lost benefits through fraud actually costs SNAP agencies $3.85 based on additional costs related to labor and administrative activities. This is up from $3.72 in 2022. For SNAP agencies that have more multi program responsibility and an above average level of mobile based applications, every $1 value of SNAP benefits lost through fraud is actually $4.05.[10]

The distribution of SNAP fraud losses is similarly represented by **suspicious cases not worked**, inadvertent household errors (IHEs) that have not been formally designated as an intentional program violation but **could reasonably be assumed as fraud** and electronic benefits transfer (EBT) skimming/account take over.[10]

In 2022, one state alone experienced an approximate **loss of $338,000 via EBT card skimming**; however, in the first half of 2023, the reported amount is already up to $1,342,000.[11]

MITIGATION STRATEGY: A trusted, secure identity verification workflow that allows for equitable access while deterring fraud is crucial for SNAP agencies. Couple the front-end verification with a back-end investigative solution to catch fraudsters already lurking in your SNAP population. Educate recipients on secure pin numbers to prevent easy guessing by bots in EBT card skimming.

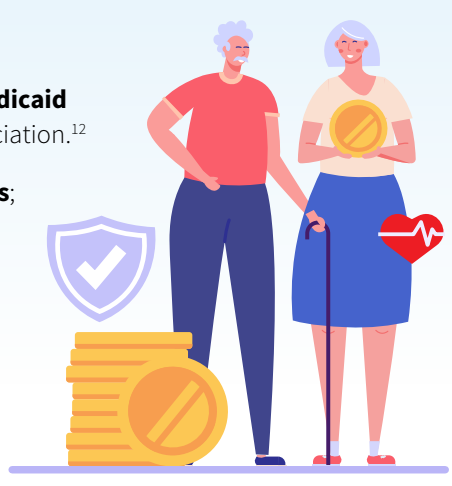
5. Medicare & Medicaid Fraud

Medicare and Medicaid fraud are illegal practices aimed at obtaining high payouts from government-funded healthcare programs. Bad actors who exploit these programs can cost taxpayers billions of dollars while putting beneficiaries' health and welfare at risk. The impact of these losses and risks magnifies as Medicare continues to serve increasing numbers of beneficiaries.

Taxpayers are losing more than $100 billion a year to Medicare and Medicaid fraud, according to estimates from the National Health Care Anti-Fraud Association.[12]

Medicare spends about $901 billion a year on its **65 million beneficiaries**; **Medicaid spends $734 billion** providing medical coverage to more than **85 million** poor and disabled Americans every year, according to the Centers for Medicare and Medicaid Services (CMS).[14]

According to the CMS, the **Medicaid improper payment rate was 15.62% or $80.57 billion** in 2022.[14]



MITIGATION STRATEGY: Verify Medicare and Medicaid Providers at point of entry to mitigate risks entering the system. Conduct continuous monitoring for licensure and sanction changes to identify new risks and avoid continued payments to bad actors and ineligible providers.

LexisNexis® Risk Solutions can help. Learn about how our solutions can help your agency battle evolving cyber and fraud risk.

LexisNexis® RISK SOLUTIONS

Scan the QR code or call us at 1.888.216.3544

1. https://www.sdxcentral.com/articles/news/synthetic-identity-fraud-is-at-an-all-time-high-how-does-it-work/2023/08/
2. https://www.aarp.org/money/scams-fraud/info-2022/dmv.html
3. https://6abc.com/drivers-licenses-identity-theft-uber-resource-center/13359251/
4. https://www.cnbc.com/2023/09/15/student-loan-borrowers-at-risk-of-scams-as-payments-restart-says-ftc.html
5. https://www.forbes.com/sites/emmawhitford/2022/11/03/student-loan-scams-stole-an-estimated-5-billion-from-americans-this-year/?sh=4badbf6766f5
6. https://finance.yahoo.com/news/student-loans-2023-3-scams-233637002.html
7. https://www.securitymagazine.com/articles/99807-social-security-numbers-were-exposed-in-69-of-breaches-in-2023
8. https://www.newsweek.com/social-security-scams-money-lost-1851415#:~:text=More%20than%20%24100%20million%20is,the%20most%20common%20of%20all
9. https://www.latimes.com/business/story/2023-11-25/how-to-spot-social-security-scams-and-protect-your-identity
10. https://risk.lexisnexis.com/insights-resources/infographic/discover-fraud-cost-for-snap-and-ies-agencies
11. https://www.thomsonreuters.com/en-us/posts/government/government-benefits-fraud/
12. https://www.forbes.com/sites/forbestechcouncil/2023/09/20/how-medicare-and-other-fraud-in-the-us-can-be-prevented/?sh=3e1294a33c46
13. https://www.cnbc.com/2023/03/09/how-medicare-and-medicaid-fraud-became-a-100b-problem-for-the-us.html
14. https://www.sas.com/content/dam/SAS/documents/briefs/solution-brief/en/detect-prevent-medicaid-fraud-107258.pdf

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.