



FRAUD DETECTION AND MITIGATION: A TECHNOLOGY-DRIVEN AND RISK-INFORMED PERSPECTIVE FOR TODAY'S EVOLVING THREATS

TABLE OF CONTENTS

Introduction	4
Common Fraud Types	6
Fraud Detection Techniques and Practices	8
Fraud Risk Mitigation	13
Harnessing Artificial Intelligence (AI) in Fraud Detection and Mitigation	17
Conclusion	19

Disclaimer:

This white paper was prepared by the ATARC Fraud Detection and Mitigation Working Group members in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated.

Acknowledgments

ATARC would like to take this opportunity to recognize the following Fraud Detection and Mitigation Working Group members for their contributions:

Eric Rivera, EXIM, ATARC Fraud Detection and Mitigation Working Group, Government Chair
Bobby Duffy, nForce AI, ATARC Fraud Detection and Mitigation Working Group, Industry Chair
Arjuna Swaminathan, U.S. Department of Health & Human Services (HHS)
Ferdous Khan, U.S. Department of Homeland Security (DHS)
Rebecca Shea, US Government Accountability Office (GAO)
Sherese Shy-Holmes, U.S. Railroad Retirement Board, Office of Inspector General (OIG)
Vince Sprouls, GrantSolutions
Henry Sienkiewicz, Georgetown University
Pat Pulliam, Recorded Future
Jordan Burris, Socure
Mike Cook, Socure
Chris Hill, Socure
Jennifer Kerber, Socure
Nick Oppelt, Nuix
Jennifer Weaver, LexisNexis Risk Solutions
Jacob Weise, ID.me
Luke Wolf, ID.me
Gareth Barendse, ID.me
Wes Turbeville, ID.me
Greg Crabb, 10-8
Aaron Pujanandez, Delta Lima
Steve Ryan, Steve Ryan Law
Merrick Krause, ATARC Working Group, Member
Mary Grace "MG" Karch, Ntrepid
Steve Brady, Bison Technology Services

1 INTRODUCTION

Fraud is a deliberate act of deception for unlawful gain. It thrives in environments marked by ambiguity, scale, and speed; especially where financial resources are involved. Fraud takes root in systems lacking consistent oversight, standardized processes, and timely detection mechanisms.

According to the Government Accountability Office (GAO), the federal government loses an estimated \$233 billion to \$521 billion annually to fraud.¹ This represents 3 - 7 percent of all federal spending and does not include fraud losses that impact state, local, and tribal governments. During the Coronavirus Pandemic, in the face of large government stimulus programs rushing desperately needed relief to individuals and businesses, the fraud was even higher, with one private sector company estimating losses to be \$1 trillion.²

Fraudsters are indiscriminate in selecting government programs to attack. Nearly every federal benefits program sees different types of fraudsters trying to beat the design, eligibility, and systems for each program:

Department of Labor (DOL) Unemployment Insurance - GAO estimates that the amount of fraud during the pandemic is likely between \$100 billion and \$135 billion.³ But that is likely understated. Independent private sector estimates are in the \$350-400 billion range.^{4,5,6}

Federal Emergency Management Agency (FEMA) - DHS's Office of the Inspector General (OIG) reports fraud across nearly all of FEMA's programs:

Disaster Assistance: Eighteen OIG audits between 2019 and 2023 found \$3.9B in improper payments across Disaster Assistance Programs, including

- overpayments, ineligible payments, and unallowable costs.⁷

Lost Wages Assistance (LWA) Program: The OIG identified over \$3.7 billion in improper payments related to the LWA program, with \$3.3 billion

- potentially fraudulent.⁸

Home Repair Assistance: The OIG questioned more than \$3 billion in improper and potentially fraudulent payments made through FEMA's

- Individuals and Households Program (IHP) for home repairs since 2003.⁹

Centers for Medicare and Medicaid Systems (CMS) - In 2024, GAO reported that Medicare and Medicaid account for roughly half of the \$236 billion in improper payments across federal programs. The Trump Administration began taking action, with Department of Justice announcing a largest-ever shakedown with 324 defendants linked to \$14.6 billion in fraudulent losses.¹⁰

Pandemic Response Accountability Committee (PRAC) - In a June 2025 fraud alert report, the PRAC focused on some of the largest pandemic relief programs: the Small Business Administration's (SBA) COVID-19 Economic Injury Disaster Loan (COVID-19 EIDL) program and Paycheck Protection Program (PPP), and the DOL's pandemic-related Unemployment Insurance (UI) programs. In 2023, the SBA OIG and the DOL OIG estimated that the total amount of fraud and improper payments for these programs is nearly \$400 billion. In this alert, the PRAC estimates the amount of potential fraud across these programs stemming from the use of stolen or invalid Social Security numbers (SSNs), and illustrates how pre-award vetting using the PRAC's data analytics tools could have mitigated this risk.^{11,12,13}

The picture is equally stark in the private sector as well. In July of 2024, Treasury’s Financial Crimes Enforcement Network (FinCEN) director, Andrea Gacki, reported that 69% of all synthetic activity by volume (1.7M) and 57% by value (\$200B) are related to “Impersonation”: false records, scams, and synthetic identity at account creation.^{14,15,16} Just a year earlier, impersonation accounted for only 40% of synthetic activity.

Beyond the financial impacts, identity theft also extracts a significant emotional toll on victims. According to the Identity Theft Resource Center, the percentage of identity theft victims who contemplate suicide doubled from 8% to 16% from 2020 to 2022.¹⁷

This white paper proposes a standardized, risk-based, and technology-driven model for fraud detection and prevention across U.S. government agencies. Aligned with the GAO’s Fraud Risk Framework, the model supports a proactive approach to fraud risk management.

The COVID-19 pandemic underscored the urgency of this approach. Emergency relief programs, including the PPP and expanded unemployment insurance, were deployed rapidly, often with relaxed controls to expedite assistance. This speed and scale created gaps that fraud actors exploited, leading to billions in improper payments. These failures revealed critical weaknesses in identity verification, application vetting, data-sharing, and real-time monitoring.

According to a recent Government Fraud Patterns Report¹⁸, recent analyses of digital fraud trends have uncovered coordinated attacks against U.S. government programs by both domestic and international fraud rings. These operations often involve the rapid reuse of stolen identities, the deployment of synthetic identities with fabricated digital footprints, and the manipulation of email, phone, and IP address infrastructure, demonstrating a high degree of organization and adaptability. These findings underscore the urgent need for standardized, technology-enabled fraud detection frameworks across agencies.

Fraud erodes public trust, diverts essential resources, and weakens the effectiveness of public programs. As agencies continue to manage high-volume operations, ranging from pandemic response and disaster recovery to long-term entitlement programs, a coordinated, strategic model is essential.

The model outlined here is modular and adaptive, supporting different fraud types and program maturities. It applies consistent principles across various initiatives, whether administering emergency funding or ongoing benefits like Medicaid and Social Security. By emphasizing the four key stages in the customer journey: application, verification, disbursement, and post-payment review, it promotes tailored controls throughout the program lifecycle. The ultimate goal is to equip agencies with tools, data, and governance structures to safeguard integrity and accountability in public service delivery.

While the scale of government fraud is staggering, its complexity lies in the diverse tactics fraudsters use to exploit vulnerabilities. Understanding these tactics is the first step toward crafting effective defenses.





2 COMMON FRAUD TYPES

Government programs face diverse fraud types, each requiring specific strategies. The GAO's fraud ontology categorizes these fraud types by program, helping agencies apply the right tools and strategies based on their risk profiles.

Identity theft - Identity theft is widespread, with fraudsters using stolen or false identities to claim benefits. Digital applications and remote verification increase this risk in programs like Social Security, Medicaid, and unemployment insurance.

- There are three basic types of identity fraud, depending on the relationship between the fraudster and the person or information they are attempting to exploit.

	DEFINITION	EXAMPLE
FIRST party fraud	The actual owner of the identity commits the fraudulent act.	Individual creates accounts to apply for unemployment from multiple workforce agencies.
SECOND party fraud	A representative of the owner of the identity commits the fraudulent act e.g. attorney caretaker, doctor.	Nurse assistant steals their patient's identity to create an IRS account and steal tax returns.
THIRD party fraud	A person unrelated to the owner of the identity used commits the fraudulent act.	An unrelated individual offers someone a fake job opportunity to collect their identity information.

Figure 1: Types of identity fraud

Payment fraud - Payment fraud is any illegal or unauthorized transaction using a payment method. It can be first, second, or third-party fraud and includes falsified applications, forged signatures, and manipulation of digital payment systems. COVID-era relief programs like the PPP were especially vulnerable to such abuse.

Procurement fraud - Procurement fraud involves collusion, overbilling, and kickbacks. Due to complexity and volume in contracting, these schemes often go undetected.

Emergent fraud - Emergent fraud evolves rapidly in new or temporary programs like disaster relief or emergency grants, often outpacing detection systems.

Ongoing fraud - Ongoing fraud refers to long-established scams, such as falsified disability claims or long-term benefit abuse, sometimes with insider involvement.

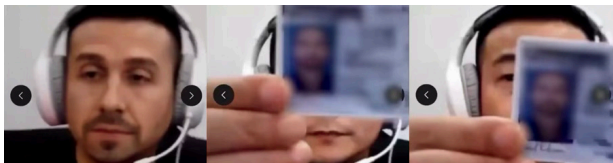


Figure 2: Deepfakes have been used to impersonate individuals using their stolen information and images of their driver's licenses; there are ways to disrupt these attacks (source: ID.me)

Generative Artificial Intelligence (GenAI) and deepfakes have emerged as a fraud accelerant. While these tools have not created new types of fraud, they have made it easier for fraudsters to create more effective schemes and harder for antifraud measures to differentiate fraudster from legitimate actors. Deepfakes and AI-generated media, also known as synthetic media, are rapidly evolving technologies with significant societal implications. Deepfakes, specifically, are manipulated videos, audio, or images created using AI to convincingly replace one person's likeness with another, making them appear authentic. A recent 60 minutes report¹⁹ dove into the rise of deepfakes impersonating individuals engaging call centers and remote identity verification processes. Effectively countering and staying ahead of these fraud types requires an ever evolving range of tools and techniques. Recognizing the different types of fraud is only half the battle; responding effectively requires tools and systems designed to spot trouble before it takes root.


3 FRAUD DETECTION TECHNIQUES AND PRACTICES

Fraud detection in government has evolved significantly through technology and increasingly sophisticated schemes. Agencies now rely on tools ranging from traditional rule-based systems to advanced artificial intelligence (AI) and machine learning (ML) and biometrics. These methods allow for real-time analytics, anomaly detection, and predictive modeling, enabling faster identification of suspicious activities.

AI refers broadly to systems designed to replicate human decision-making, while ML, its data-driven subset, learns from past behavior to detect fraud patterns without being explicitly programmed for each case. These tools are now used across a range of programs to assess risk, flag irregularities, and optimize responses. Biometrics refers to the automated recognition of individuals based on their biological and behavioral characteristics, such as an image of their face or the way they type on a keyboard.

While all of these methods are powerful tools for fraud detection, their effectiveness is fundamentally limited by the quality and availability of data. Many agencies operate in data silos, with fragmented systems that lack interoperability. This prevents AI models and other tools from accessing the full spectrum of fraud signals, leading to blind spots and reduced accuracy.





In addition, poor data quality degrades model performance, increases false positives, and erodes trust in automated systems. In many cases, government agencies rely on legacy systems (GAO-25-107795) that were not designed for modern analytics, making it difficult or impossible to train supervised models or validate effectiveness or detection outcomes. Common data issues include:


- Incomplete data (e.g. missing fields in benefit applications)
- Outdated data (e.g. deceased individuals still listed as active beneficiaries)
- Inconsistent data (e.g. different formats for names, addresses, or dates across systems)
- Unlabeled (e.g. no indication of whether a transaction was fraudulent or not)

These challenges are compounded when fraud prevention systems are deployed independently across agencies without shared standards or governance. Siloed fraud prevention systems may duplicate efforts, miss fraud patterns, or even produce conflicting risk assessments for the same individual or entity.

To address these issues, government agencies should:

- Conduct data readiness assessments before deploying fraud detection tools
- Invest in data standardization and cleansing initiatives
- Break down silos through secure sharing
- Leverage private-sector partnerships and best practices
- Invest in metadata and labeling

Without complete and accurate data, even the most advanced AI and fraud prevention programs will fall short of their potential. A coordinated and data-first approach is essential to unlocking the full value of the tools discussed throughout this paper.



GAO has developed a comprehensive fraud taxonomy that classifies schemes based on program type. This helps agencies align detection tools with specific risks, for example, those found in emergency grants, Social Security, or vendor fraud. Other technological enhancements include voice biometrics for identity verification and the use of open-source intelligence (OSINT) and publicly available information (PAI) to gather threat indicators from external sources. To support fraud and threat detection, the government and industry are also adopting a range of technological enhancements. These include voice and behavioral biometrics or identity verification, document validation technologies, commercial consortium fraud databases, and device analytics. Additionally, the use of OSINT and PAI allows for the proactive gathering of threat indicators from external sources.

The Department of Justice's COVID-19 Fraud Enforcement Task Force, for instance, used OSINT to prosecute a social media-based advance-fee scam targeting elderly victims. In another example, the Department of the Treasury used ML in FY2024 to detect and recover over \$4 billion in fraudulent check payments.

While these advances have increased fraud detection capabilities, effectiveness remains limited by fragmented systems and inconsistent data-sharing between agencies and private-sector partners. To address this, the white paper proposes a U.S. Government Fraud Information Sharing and Analysis Center (ISAC), modeled after similar entities in cybersecurity and finance. The ISAC would facilitate secure collaboration, sharing of fraud signals, and development of cross-agency AI models.

In shaping these tools and collaborations, it is critical that the U.S. government and its partners prioritize fraud prevention and response using a principled, risk-based methodology that accounts not just for monetary losses, but also broader programmatic and national harm. This is where the **Return on Assets Employed (ROAE)** concept and **two key hierarchies of prioritization**²⁰ are essential.

At the policy level, agencies and contractors must balance finite resources to maximize ROAE; not just in terms of financial impact, but by recognizing the severity of non-monetary harm. Certain frauds, while less costly in dollars, have greater implications for public trust, national security, or operational continuity.

The first hierarchy organizes fraud by **source**, in descending order of government priority:

- 1 Fraud by transnational criminal groups sponsored by foreign governments.
- 2 Fraud by foreign criminal groups not linked to a state.
- 3 Fraud by domestic organized criminal groups.
- 4 Program fraud by domestic business entities (e.g., Medicare fraud by providers).
- 5 Fraud committed by individuals.

The second hierarchy considers impact/severity, especially non-financial consequences:

- 1 Frauds causing the greatest programmatic or fiscal harm to the U.S. government.
- 2 Frauds that threaten the operational viability of government programs or public confidence.
- 3 Fraud that threatens finances or operations of an organization. (e.g. stealing millions in federal grants awarded to an academic institution or clinical researcher)
- 4 Fraud that threatens finances of an individual or beneficiary. (e.g. changing the direct deposit on a Social Security account)

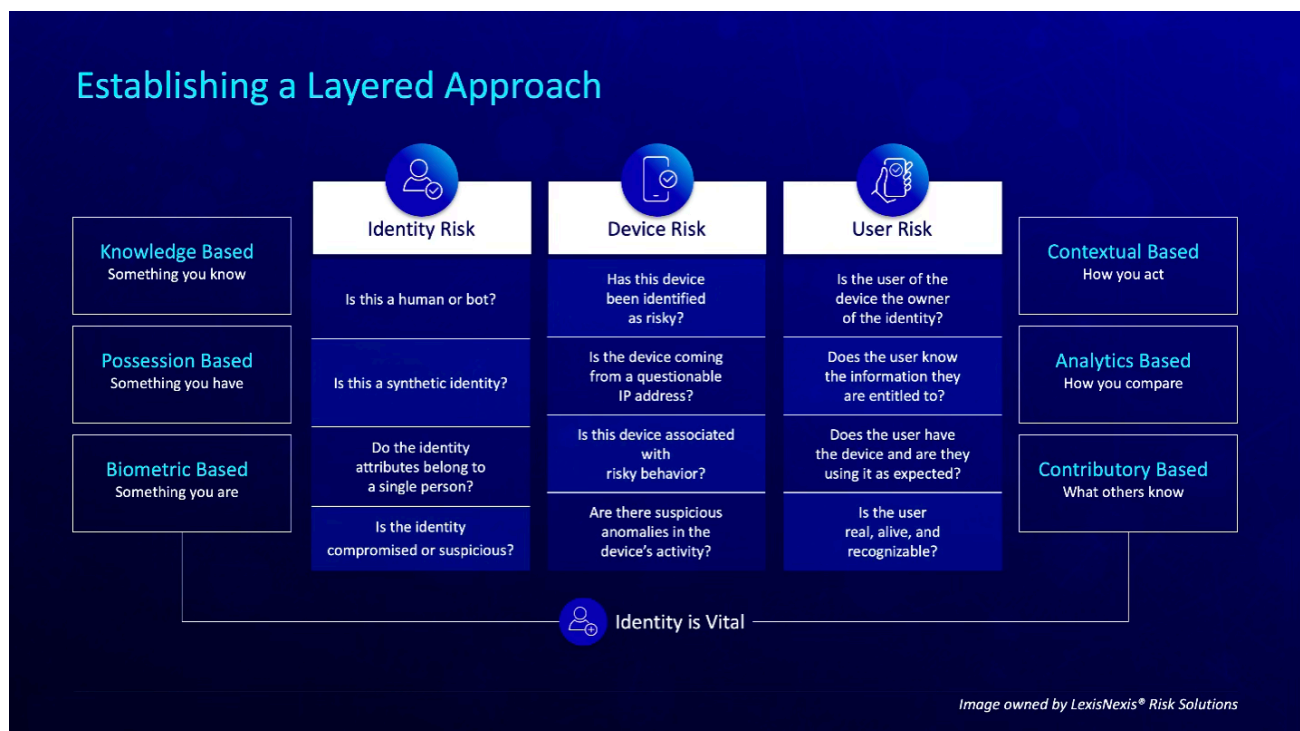


Figure 3: Establishing a Layered Approach

An illustrative case is the **PRC's cyberattack on the Office of Personnel Management (OPM)**, where over 22 million security clearance files were stolen. This attack fits the highest tier of both hierarchies: it was perpetrated by a foreign government, and the harm extended beyond data loss to national security risks and long-term institutional damage. A key contractor, USIS, self-detected an earlier breach and alerted authorities, yet was later restricted from classified work, leading to a breakdown in background investigations across federal agencies.

This example underscores why detection models and fraud prioritization frameworks must account for both the **source and severity** of fraud, not merely dollar value. No policymaker would dispute that such breaches demand elevated and immediate attention. Tools like AI and ISAC collaboration are vital, but they must be guided by a thoughtful, principled structure that weighs both financial and strategic harm.

In sum, modern fraud detection requires not only smarter tools, but a layered approach to detection and smarter priorities; driven by impact, informed by threat source, and aimed at maximizing both monetary and non-monetary return on government assets and public trust.

Using the questions in the illustration below can help government agencies determine what risks and controls to consider when building a layered approach to fraud prevention.

Considering identity, device, and user risks when building workflows enables streamlined user experiences and maximum fraud detection. The illustration below shows a Sample Application Workflow that assesses the risks of an applicant in a real-time and automated manner.

Even the most sophisticated detection tools are only as effective as the systems and strategies that support them. Ensuring those systems are aligned and responsive is essential to turning detection into prevention.

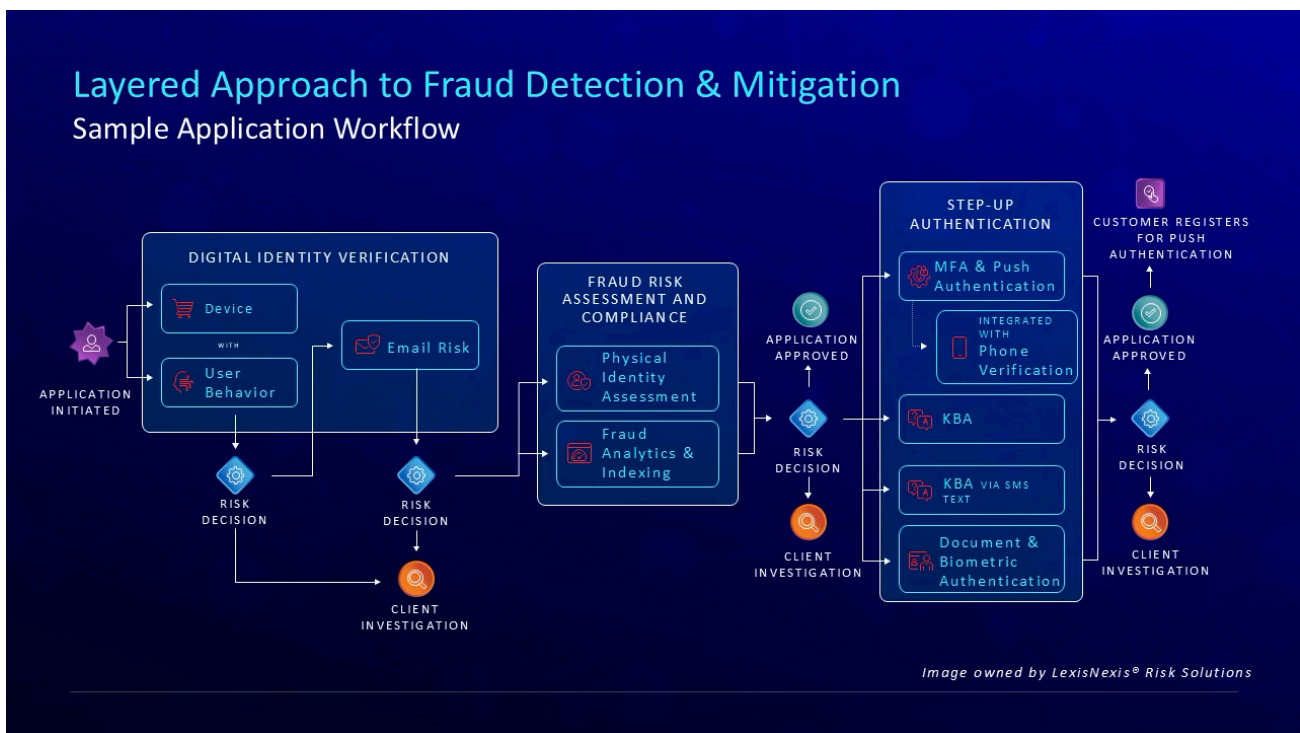


Figure 4: Layered Approach to Fraud Detection and Mitigation

FRAUD RISK MITIGATION

Effective payment fraud mitigation requires comprehensive, risk-based controls across the entire customer journey, from initial application through benefit disbursement, to post-payment review. Key risk points such as identity verification, payment processing, and vendor transactions must be secured with preventative controls to reduce fraud attempts and minimize potential losses.

However, several persistent challenges remain. These include fragmented data systems, inconsistent fraud policies, and limited avenues for victim restitution or whistleblower protection, and a general lack of shared standards. Individuals defrauded through identity theft often face unresolved harm, while whistleblowers encounter struggle with bureaucratic barriers that deter reporting.

To address this, agencies should adopt GAO-aligned frameworks that incorporate fraud oversight, routine risk assessments, and program-level controls. Public-private partnerships are also critical, bringing in financial sector expertise, data-sharing capabilities, and technical resources. To be effective and accountable, private-sector partners must not only deliver technical solutions but also adhere to public-sector standards for transparency, interoperability, and risk alignment.



Equally critical is the establishment of consistent fraud definitions and labeling strategies. Many agencies lack the infrastructure to categorize fraud accurately, such as synthetic identity fraud, third-party fraud, payments fraud, or check fraud, therefore limiting their ability to detect patterns or prioritize response efforts. Defining and labeling fraud types consistently across federal and state levels will support more targeted risk modeling, resource allocation, and training.

Structured reporting plays a pivotal role in reinforcing this approach. Regular, standardized reporting not only reinforces definitional consistency but also fosters transparency and accountability. As fraud metrics are tracked across programs and jurisdictions, this creates a natural incentive structure, a form of healthy competition, that encourages continuous improvement. *After all, you can't reduce what you don't measure, and you can't measure what you don't define.*

Finally, training is vital. Program staff must receive regular fraud awareness instruction, and joint training initiatives with private-sector experts can help build cross-cutting resilience. Agencies must also continuously monitor fraud activity and evolve their strategies in response to new threats and tactics.

With proper frameworks and best practices in place, modern security technologies like AI-powered tools can serve as force multipliers for program staff. These solutions help detect payment fraud proactively by providing visibility into full risk exposure, particularly when both personally identifiable information and payment data are compromised.

To maximize effectiveness and value of their IT investments, agencies should prioritize payment fraud prevention tools that integrate with existing systems and infrastructure. At the intersection of innovation and necessity lies a powerful ally: AI. As fraud grows more adaptive, so too must the tools we use to fight it.



5 HARNESSING ARTIFICIAL INTELLIGENCE (AI) IN FRAUD DETECTION AND MITIGATION



AI and ML offer transformative capabilities for detecting and preventing fraud. Unlike traditional systems, these models adapt and improve over time, identifying evolving fraud schemes with speed and precision.

AI enables automated reasoning and language analysis, while ML builds predictive models based on past data. These technologies power real-time analytics, anomaly detection, and identity verification using tools like biometrics, including voice, and OSINT.

To combat increasingly sophisticated fraud, including the rise of synthetic identities and deepfakes, agencies must deploy layered defenses. This includes leveraging device intelligence and behavioral analytics, which analyze how a user interacts with systems (e.g., typing cadence, mouse movement, mobile sensor signals) and the devices they use. These behavioral and device-based signals add an invisible layer of verification that is hard for fraudsters to replicate.

Deepfakes and AI-generated identity fraud present a growing risk. To counter these threats, ML models must be trained specifically to detect manipulated images, videos, and synthetic speech. These tools can identify subtle irregularities that signal the presence of deepfake media, especially when paired with behavioral anomaly detection and hardware signal analysis.

However, success depends on access to quality data and inter-agency collaboration. Siloed systems and inconsistent data limit the accuracy and effectiveness of AI models. Public-private partnerships are essential to overcome these gaps through shared intelligence and collaborative model development.

AI models must also be continuously retrained to respond to emerging tactics. Fraudsters move quickly, and static models become obsolete. Agencies must prioritize adaptive learning and refinement to maintain relevance and reduce false positives.



When it comes to the use of biometrics, agencies take different approaches, with some using them extensively and some putting limitations on their use. As GenAI and deepfakes advance in quality, the only way to stop fraud will be by layered defenses. Best practice includes applying both biometrics and AI/ML to stop identity fraud and AI/ML to find and mitigate other types of fraud. Best practice includes combining biometrics, behavioral analytics, device intelligence, and AI/ML models, each providing unique signals, to verify identity and detect anomalies. As agencies expand their use of biometric and behavioral analytics, *it is essential to balance innovation with the preservation of individual privacy and civil liberties.*

To maximize impact, government agencies should adopt standardized AI/ML models and approaches to the use of biometrics, coordinated by the Office of Management and Budget (OMB) and aligned to GAO's ontology, allowing consistent fraud detection across programs and enabling shared learning. Technology may provide the scaffolding, but the foundation of fraud prevention rests on coordination, policy, and people. As we consider what's possible, we must also commit to what's essential.

A crucial factor in utilizing AI to combat fraud is avoiding the simple replication of existing models. Firms often overlook a vital element: deep technical integration. It's essential to foster public and private partnerships to establish a Center of Excellence, enabling the co-creation of solutions rather than merely reselling software. Begin by identifying an AI fraud use case and defining the specific business problem. Build the technical solution around this problem, aiming to deliver immediate value. Once effective solutions are established, focus on scaling them. In today's fraud landscape, successfully harnessing AI depends on a strong execution philosophy.

6

CONCLUSION

Fraud remains a serious threat to government programs, compromising financial resources and public confidence. This white paper recommends a standardized, OMB-directed, GAO-aligned model for proactive fraud detection and prevention, supported by technology and collaboration.

AI, ML, biometrics, and OSINT tools offer powerful capabilities to detect fraud in real-time, but their effectiveness relies on agency cooperation, consistent application, and private-sector partnerships. These relationships provide access to fraud signals, behavioral analytics, and technical infrastructure that government agencies alone may lack.

Equally important are training and public awareness. Educating government staff and empowering the public to report fraud are critical steps toward early detection and prevention. Open reporting channels and whistleblower protections help build a more fraud-resilient environment.

A successful strategy requires integrated frameworks, modern technology, and unified efforts across sectors. With sustained commitment to these principles, agencies can strengthen defenses, improve program integrity, and protect public trust.



References:

1. U.S. Government Accountability Office (GAO). Fraud Risk Management: Federal Agencies Estimated Annual Losses from Fraud Ranged from \$233 to \$521 Billion. GAO-24-105833. <https://www.gao.gov/products/gao-24-105833>
2. U.S. House Committee on Ways and Means. Testimony of Haywood Talcove, CEO, LexisNexis Risk Solutions Government Group. January 2025. <https://waysandmeans.house.gov/wp-content/uploads/2025/01/Talcove-Testimony.pdf>
3. U.S. Government Accountability Office (GAO). COVID-19 Relief Funds: Agencies Reported Fraud, Waste, and Abuse. GAO-23-106696. <https://www.gao.gov/products/gao-23-106696>
4. Heritage Foundation. Rachel Greszler Testifies to Congress on Unemployment Insurance. 2021. <https://www.heritage.org/impact/heritage-fellow-rachel-greszler-testifies-congress-unemployment-insurance>
5. Axios. Pandemic unemployment fraud may have stolen \$400 billion in benefits. June 10, 2021. <https://www.axios.com/2021/06/10/pandemic-unemployment-fraud-benefits-stolen>
6. Axios. Pandemic unemployment fraud may have stolen \$400 billion in benefits. June 10, 2021. <https://www.axios.com/2021/06/10/pandemic-unemployment-fraud-benefits-stolen>
7. U.S. Department of Homeland Security, Office of Inspector General (OIG). Testimony of Deputy Inspector General Kristen D. Bernard before the U.S. House of Representatives. March 12, 2024. <https://www.oig.dhs.gov/sites/default/files/assets/TM/2024/testimony-deputy-inspector-general-kristen-d-bernard-march-12-2024.pdf>
8. U.S. Department of Homeland Security, Office of Inspector General (OIG). FEMA Should Recover \$3.9 Billion in Improper Payments Made Under Disaster Assistance Programs. OIG-22-69. September 2022. <https://www.oig.dhs.gov/sites/default/files/assets/2022-09/OIG-22-69-Sep22.pdf>
9. U.S. Department of Homeland Security, Office of Inspector General (OIG). FEMA's Individuals and Households Program Was Susceptible to Significant Fraud and Improper Payments. OIG-20-23. April 2020. <https://www.oig.dhs.gov/sites/default/files/assets/2020-04/OIG-20-23-Apr20.pdf>
10. U.S. Department of Justice (DOJ). National Health Care Fraud Takedown Results in Charges Against 324 Defendants Involving Over \$146 Billion in False Billings. 2021. <https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-324-defendants-charged-connection-over-146>
11. Pandemic Response Accountability Committee (PRAC). Official Website. <https://pandemicoversight.gov/>
12. Pandemic Response Accountability Committee (PRAC). Fraud Prevention Alert Report. June 2025.
13. Pandemic Response Accountability Committee (PRAC). Semiannual Report to Congress. October 1, 2024 – March 31, 2025.
14. U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN). Synthetic Identity Fraud Infographic. April 2023. https://www.fincen.gov/sites/default/files/shared/FinCEN_Infographic_Public_2023_April_21_FINAL.pdf
15. American Bankers Association (ABA) Banking Journal. Synthetic Identity Fraud Results in \$20 Billion in Losses in 2020. October 2021. <https://bankingjournal.aba.com/2021/10/report-synthetic-identity-fraud-results-in-20-billion-in-losses-in-2020/>
16. U.S. Department of the Treasury, Financial Crimes Enforcement Network (FinCEN). Prepared Remarks at Identity Project Colloquium. June 2024. https://www.fincen.gov/sites/default/files/2024-06/PREPARED-REMARKS-IDENTITY-PROJECT-COLLOQUIUM-FINAL-508_0.pdf
17. Identity Theft Resource Center (ITRC). 2023 Consumer Impact Report: Record-High Number of Victims Report Suicidal Thoughts. 2023. <https://www.idtheftcenter.org/post/2023-consumer-impact-report-record-high-number-itrc-victims-suicidal-thoughts/>
18. Socure. Government Fraud Patterns Report. July 2025. <https://media.socure.com/app/uploads/2025/07/GovernmentFraudPatternsReport.pdf>
19. CBS News – 60 Minutes. “Fraud.” Season 57, Episode 33. Original air date: May 11, 2025. <https://www.it.miami.edu/about-umit/it-news/phishing/deepfakes/index.html>
20. U.S. Government Accountability Office (GAO). Medicare and Medicaid: Improper Payments Continue to Be Widespread. GAO-12-688. 2012. <https://www.gao.gov/assets/690/687046.pdf>