IBM Center for The Business of Government

2025

ENHANCING GOVERNMENT PAYMENT INTEGRITY

Leveraging AI and Other Emerging Technologies

With contributions from

Richard Hoehne
Georgia State University

Dr. Karen Kunz
West Virginia University

National Academy of Public Administration

IBM Center for The Business of Government

Enhancing Government Payment Integrity: Leveraging AI and Other Emerging Technologies

With contributions from

Richard Hoehne
Georgia State University

Dr. Karen Kunz
West Virginia University

FEBRUARY 2025

IBM Center for
The Business of Government

TABLE OF CONTENTS

Foreword 4

Executive summary 6

Introduction 8

Part 1—The Overall Landscape 11
- Discussion Topic One: Challenges 12
- Discussion Topic Two: Opportunities For Improvement 15
- Discussion Topic Three: Next Steps 22
- Conclusion 24

Part 2—Detailed Roundtable Discussion Summary 25
- Discussion Topic One: Challenges 26
- Discussion Topic Two: Lessons Learned 28
- Discussion Topic Three: Next Steps 30

Appendix 32

About the Authors 33

Recent Reports from the IBM Center for The Business of Government 35

FOREWORD

On behalf of the IBM Center for The Business of Government, we are pleased to present this new report, *Enhancing Government Payment Integrity: Leveraging AI and Other Emerging Technologies*, by contributing authors Richard Hoehne, Georgia State University, and Karen Kunz, West Virginia University.

In an era where technological advancements are rapidly transforming the economy, the integrity of government benefit and payment systems has become a critical concern. Agencies must address the multifaceted challenges and opportunities associated with advancing payment integrity by adopting innovative solutions, including artificial intelligence (AI), to combat improper payments—which can include fraud, waste, or abuse.

This new report draws on insights from an expert roundtable to provide a comprehensive overview of the current landscape, the hurdles faced by agencies, and the potential pathways to enhance payment integrity. The first part of the report focuses on the overarching challenges facing agencies in their efforts to reduce improper payments, especially through leveraging AI and other emerging technologies. These challenges range from restrictions on data sharing and outdated laws, to the lack of consistent incentives and the rapid evolution of technology used by adversaries. The discussion underscores the complexity of balancing identity protection with customer experience, and the difficulties posed by siloed systems and inconsistent data structures.

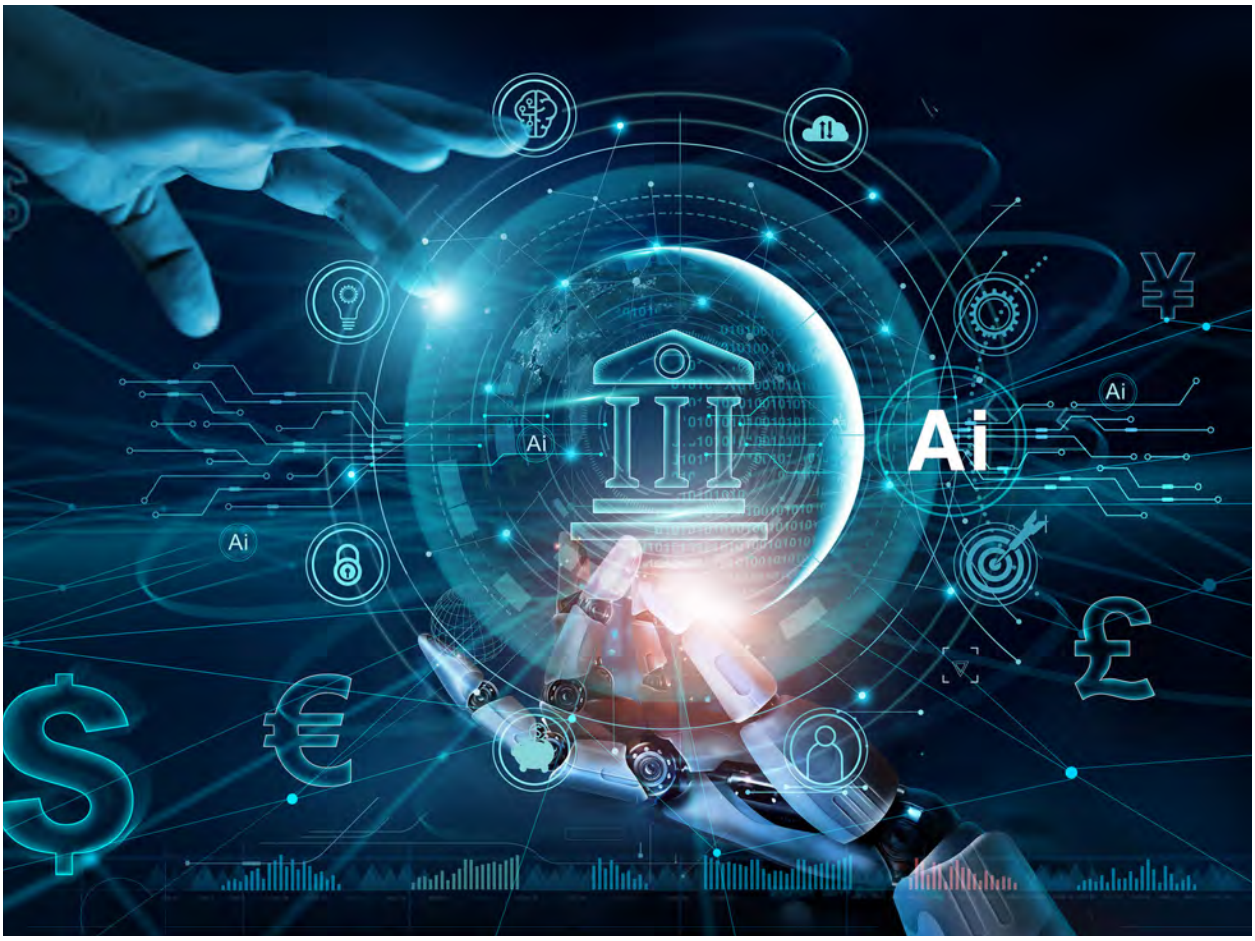
Moving from challenges to solutions, the second part of the report identifies key opportunities for improvement. Collaboration across agencies and with industry partners emerges as a crucial strategy for enhancing payment integrity. By sharing technology advances, data, and insights, agencies can develop more robust capabilities to detect and prevent improper payments. The report also highlights the importance of leveraging AI and machine learning to automate processes, improve data consistency, and enhance identity verification and fraud detection mechanisms.

The report further outlines a framework for improvement, detailing specific areas where agencies can focus their efforts. These include securing access through advanced AI-powered identity management, optimizing policies to align with modern technology, and automating processes to reduce human error. The framework also emphasizes the need for pre-payment detection, rapid response to fraud alerts, and the development of a modern data strategy. By adopting these measures, agencies can transition beyond only reactive "pay and chase" models, to proactive approaches that leverage AI to prevent improper payments before they occur.

DANIEL J. CHENOK

LAUREN CRAIG

JAMES-CHRISTIAN BLOCKWOOD



This report builds on multiple IBM Center reports that have helped government leaders to achieve success in using AI and innovative technologies to improve mission delivery, including *Digital Modernization for Government: An Implementation Framework*, *A Prepared Federal Government: Preventing Fraud and Improper Payments in Emergency Funding*, and *AI and the Modern Tax Agency*.

We hope the report serves as a valuable resource for agency leaders, providing actionable insights and strategies for using AI to enhance the efficiency and integrity of government payment systems—ultimately promoting public trust and program sustainability.

Daniel J. Chenok
Executive Director
IBM Center for
The Business of Government
chenokd@us.ibm.com

Lauren Craig
Partner, U.S. Federal
Civilian Agencies, IBM
laurenc@us.ibm.com

James-Christian Blockwood
President & CEO
National Academy of Public
Administration
JCBlockwood@napa.org

EXECUTIVE SUMMARY

In response to the pressing challenge of reducing improper payments, which amounted to $2.7 trillion over two decades, the IBM Center for The Business of Government and the National Academy of Public Administration co-hosted a roundtable in November 2024.

The event brought together federal agency leaders, congressional staff, and AI, industry, and academic experts to discuss the complexities of improving payment integrity, especially in light of increasing efficiency focus in 2025. Participants explored challenges, opportunities, and AI-driven solutions to tackle improper payments, including fraud, waste, abuse, overpayments, underpayments, and disbursements to ineligible recipients. The roundtable's insights form the basis of this report, which highlights specific issues and proposes next steps for enhancing government payment integrity using AI technology.

The first roundtable discussion highlighted several challenges faced by federal agencies in reducing improper payments, including data sharing restrictions, insufficient investment in analytics and AI, the ineffectiveness of the "pay and chase" model, and a lack of consistent and measurable incentives. No single entity in the federal government is solely focused on improper payments, and participants expressed concerns about keeping up with evolving technology used by adversaries, balancing identity protection with customer experience, and dealing with siloed agencies and outdated laws.

Three specific challenges emerged from the discussion: data complexity, technology limitations, and user experience. The complexity and variability of data across multiple agencies and programs present a significant hurdle to applying AI for reducing improper payments. Each agency operates with its own data standards, formats, and systems, making comprehensive integration and analysis challenging. Additionally, outdated legal frameworks, such as the Privacy Act of 1974, hinder modern data sharing protocols. The volume and diversity of data, along with potential biases in algorithms, further complicate efforts to identify and stop improper payments. Balancing robust identity verification with user experience is another challenge, as agencies must ensure secure login and authentication without creating unnecessary delays for legitimate users. Overly stringent security measures can deter eligible individuals from receiving benefits, especially vulnerable populations. Addressing these challenges requires not only technological upgrades but also advancements in skills, measures, motivations, and organizational culture to adapt effective practices.

Roundtable participants identified three main areas of focus to improve payment integrity in government: collaboration, data and AI, and technology.

- Collaboration across agencies, industry partners, and international organizations can enhance the identification and mitigation of improper payments. Sharing research, data, and best practices can standardize procedures and policies, reducing inconsistencies that adversaries might exploit.
- Data and AI focus on modernizing data strategies, standardizing common data structures, and defining ubiquitous controls while balancing privacy and payment integrity protection. AI can significantly enhance the accuracy and efficiency of identifying risky transactions and shifting from a "pay and chase" approach to pre-payment detection.

- The technology focus emphasizes layered defenses, combining advanced AI-driven behavior monitoring with a broader data view to detect fraud patterns. Monitoring policies for gaps can enhance data sharing and counter-fraud measures. Opportunities for improvement include accountability, a skilled workforce, and a Counter Fraud Framework outlining nine strategic areas: secure access, policy optimization, process automation, pre-payment detection, response, discovery, investigation, modern data strategy, and reporting and accountability. Implementing these strategies can significantly enhance payment integrity and reduce improper payments.

The roundtable identified numerous steps for agencies to reduce improper payments, improve efficiency, and enhance customer experience. Key recommendations include:

- Enhancing data sharing protocols through standardized procedures and systems, modernizing the Privacy Act of 1974, and developing a data/algorithm clearinghouse.
- Leveraging predictive analytics can help agencies uncover hidden trends and anomalies, enabling proactive fraud detection and enhancing payment process efficiency.
- A centralized fraud detection hub can facilitate real-time data analysis using advanced AI and machine learning technologies, identifying patterns and anomalies indicative of fraud before payments are made.
- Investing in advanced fraud detection tools.
- Utilizing machine learning for data consistency.
- Enhancing identity verification and monitoring can further improve payment integrity.
- Regular training and awareness programs for staff on the latest fraud detection techniques and AI tools are essential for maintaining payment integrity and fostering a culture of vigilance and accountability.
- Establishing clear governance and accountability structures, including designating an accountable senior official and defining roles and responsibilities, can support oversight, enforce anti-fraud measures, and track efforts to prevent improper payments.
- Collaborating with industry experts can help agencies stay updated on the latest fraud prevention technologies and practices, enabling the implementation of sophisticated fraud detection systems and optimizing resource allocation for improved overall payment integrity.

INTRODUCTION

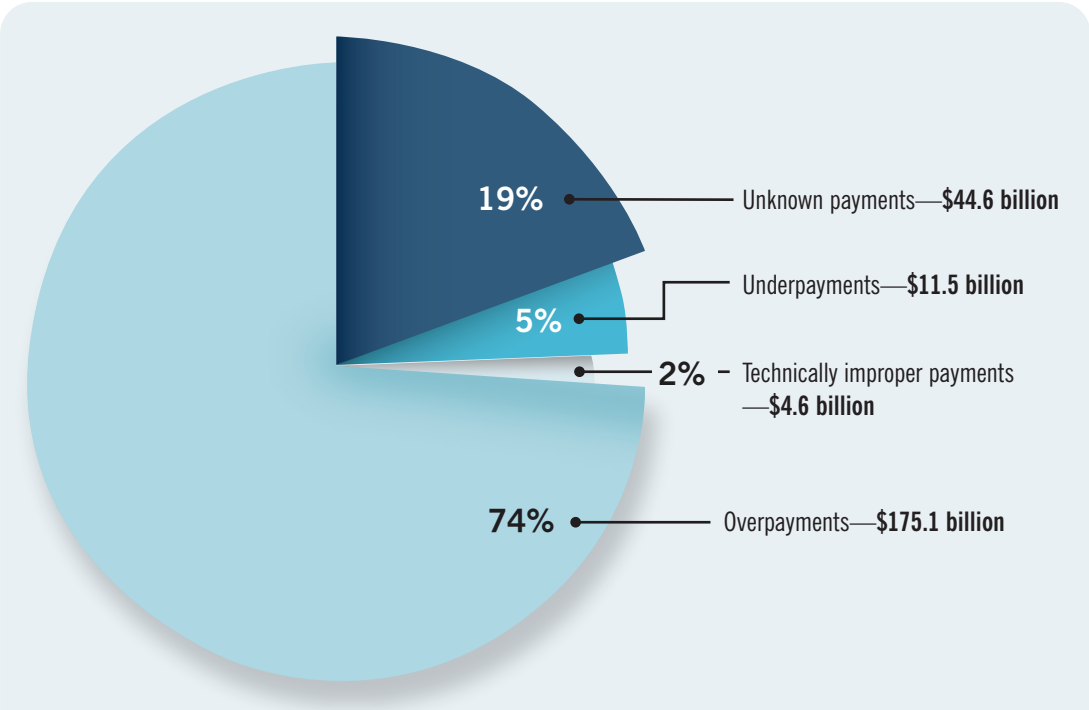
Payment integrity is an essential aspect of government accountability and transparency, two underpinnings of public trust.

With trillions spent annually, reducing improper payments is a crucial challenge for today's federal agencies. Improper—whether due to oversight, insufficient information to verify a payment, or intentional acts of fraud—divert resources from beneficiaries who are often in need, and erode confidence in government effectiveness and fiscal stability.[1] Reducing improper payments will become even more important in 2025 with the increased focus on government efficiency, as it is the one way to improve a program's solvency without reducing benefits or seeking additional funding.

To address this issue, in November 2024 the IBM Center for The Business of Government, in collaboration with the National Academy of Public Administration (the Academy), co-hosted a roundtable discussion of how artificial intelligence (AI) might be used to enhance government efforts to reduce improper payments, including fraud, waste, abuse, overpayments, underpayments, or disbursements to ineligible recipients. Leaders from agencies throughout federal government and congressional staff participated in the event. They were joined by experts from industry and academia to discuss the challenges of identity verification and lessons learned about how AI can help government to improve payment integrity.

1. Dan Chenok & Paul Dommel. "Modernizing Government Payment Systems to Improve Efficiency and Effectiveness." The IBM Center for The Business of Government Blog (December 2024). https://www.businessofgovernment.org/blog/modernizing-government-payment-systems-improve-efficiency-and-effectiveness.

Figure 1: Agency-Reported Fy 2023 Improper Payment Estimates By Type



Source: GAO analysis of Office of Management and Budget PaymentAccuracy.gov data. I GAO-24-107482

The Government Accountability Office (GAO) estimates that the federal U.S. government cumulatively made $2.7 trillion in improper payments over the past 20 years.[2] Fraud—intentional acts of misrepresentation to produce an undue financial gain—represents a part of improper payments, but not all (see Box A). As noted during the roundtable, "In FY 2023, federal agencies reported an estimated $236 billion in improper payments—ones that shouldn't have been made, were made in an incorrect amount, or lacked sufficient supporting documentation." One participant added, "The fraud you see is like an iceberg, you are only seeing what's above the surface . . . most of it is below the surface and often goes completely undetected and unnoticed."

Box A—Explaining Improper Payments

Improper payments refer to any payment that either cannot be validated or confirmed as proper. This includes payments that are made in an incorrect amount, those that shouldn't have been made at all, or those lacking sufficient supporting documentation to confirm they are proper. Improper payment can be the result of waste (over payment), abuse (receiving more than should be paid), or error (making a mistake). Fraud is the most significant form of improper payment because it is a criminal activity that uses deception or misrepresentation to produce an undue financial gain. Addressing fraud requires an additional layer of analytics to spot the fraudulent behaviors and relationships, along with improved policies, automation, and improved controls.

2. Hannah Padilla. "Improper Payments: Key Concepts and Information on Programs with High Rates or Lacking Estimates." General Accountability Office, GAO-24-107482 (June, 2024). https://www.gao.gov/products/gao-24-107482.

How much progress has been made in addressing the improper payments can be difficult to determine. Experts from the Program Integrity Alliance recently observed that "just over half of the 46 programs with available data for both 2023 and 2024 reported a reduction in improper payment *rates*. Of these, only 36 percent reduced the *actual dollar amount* of improper payments," and this only impacted the part above the surface. "Put another way, of the 64 percent of programs with *increases* in improper payment amounts, a third still managed to report decreases in their improper payment *rates* simply because their rate of spending grew faster."[3] A recent Treasury Department report also identifies additional elements of the challenges that agencies face.

Despite Size Of Opportunity, Many Agencies Are Not Advanced In Fraud Reduction Efforts

- Fraud reduction is ***perceived as being in conflict*** with the delivery of the agency's mission
- Agency leadership has ***many priorities***
- Fraud reduction is typically an ***unfunded mandate***
- Agencies ***do not know how to begin*** with fraud reduction efforts
- Agencies often ***do not possess analytics skillsets*** in house
- ***Necessary data*** can be difficult to access and inconsistent
- Existing program integrity infrastructure already ***overburdened by compliance requirements***

Source: The Department of The Treasury, Payment Integrity: Advancing the Vision Through Partnerships, Dec 4, 2024.

Using these and similar findings as a starting point, the roundtable participants came together to identify:

- Challenges to advancing payment integrity
- Opportunities on the horizon
- Next steps to best address improper payments, with an emphasis on how AI can help agencies achieve their objectives

This report draws on insights from the roundtable to lay out key issues. Following the general narrative in Part 1, Part 2 identifies specific points from the roundtable, and Appendix 1 lists roundtable organizations.

3. Linda Miller & Gavin Ugale. "Our approach to improper payments is failing; the 2024 numbers explain why." COMMENTARY | The numbers can hide what's going on. *NextGovFCW* (December 2024). https://www.nextgov.com/ideas/2024/12/our-approach-improper-payments-failing-2024-numbers-explain-why/401672/.

Part 1—The Overall Landscape

DISCUSSION TOPIC ONE: CHALLENGES

In the first roundtable discussion, participants focused on identifying the challenges that their organizations face and their efforts to reduce improper payments. They noted a variety of concerns, including restrictions on sharing data, investments in analytics (such as AI), the effectiveness of a "pay and chase model," and a lack of consistent and measurable incentives—unlike the private sector, which has a profit motive to make progress in driving innovation to reduce improper payments. Moreover, no one entity in the federal government is singularly focused on improper payments.

The participants brought their knowledge and experience to the challenge of stopping improper payments, discussing laws, limitations, and familiarity with past challenges and future opportunities. The group shared concerns with keeping up with technology and tools used by adversaries to create a dramatic increase in the volume and velocity of improper payments. Other challenges identified include balancing identity protection with customer experience, siloed agencies and systems, restrictions on sharing data, and outdated laws[4] that continue to plague payment integrity.

This discussion identified three specific challenges: data, technology, and user experience.

The Complexity and Variability of Data

The complexity, variability, and availability of data collected across the multiple agencies and programs represents a primary challenge in applying AI to reduce improper payments. Each agency often operates with its own set of data standards, formats, and systems, which can lead to challenges in integrating and analyzing data comprehensively, even in cases when regulations allow data exchange. Much of the legal framework that governs agency data sharing stems from the Privacy Act of 1974, which was developed decades ago and does not account for new and secure ways to share information. The lack of modern, standardized data sharing protocols means that every instance of data exchange can feel like "running a marathon," as one participant described. Agencies can spend months to years preparing to comply with rules to share data, and then additional time and cost to do so within the constraints provided.

Furthermore, the data itself can vary widely and encompass a wide range of information types, from financial transactions and eligibility records to behavioral data and communication logs. To gain the most from this data requires AI techniques capable of handling the scale and diversity of data sources and formats. Unfortunately, technology and tools deployed in many agencies remain outdated, and do not provide adequate support to manage such complexity within the context of approved policies. Antiquated systems and insufficient analytics capabilities hinder the potential of using AI to its full potential in identifying and stopping improper payments. Agencies struggle to process and interpret the vast amounts of data necessary for detecting improper payments.

4. Chenok & Dommel. "Modernizing Government Payment Systems to Improve Efficiency and Effectiveness." IBM Center on The Business of Government (2024). https://www.businessofgovernment.org/blog/modernizing-government-payment-systems-improve-efficiency-and-effectiveness.

> *AI systems rely on historical data to make predictions and identify patterns. . . . This can potentially lead to unfairness or inaccurate identification of improper payments, further complicating efforts to reduce fraud, waste, and abuse.*

Another concern involves the potential for biases within the data and algorithms. AI systems rely on historical data to make predictions and identify patterns, which can lead to bias in AI model outputs. This can potentially result in unfair or inaccurate identification of improper payments, further complicating efforts to reduce fraud, waste and abuse. Addressing these biases requires careful examination and curation of the data, a resource-intensive process that many agencies cannot handle without more people or improved technology.

The sheer volume of data generated by federal programs adds another layer of complexity. With trillions of dollars spent and millions of transactions processed annually, agencies face the daunting task of monitoring and analyzing this data in real-time. Solutions, including the use of AI, must scale securely to handle such large datasets, but many agencies lack the necessary infrastructure and expertise to implement and maintain these advanced technologies. This limitation presents a fundamental barrier to applying AI in order to reduce improper payments.

Transitioning to AI-driven systems requires not only technological upgrades but also advancements in skills, measures, motivations, and organizational culture to adapt effective practices. This includes training personnel, updating policies, ensuring the availability and consistency of data, and using AI tools ethically and effectively. Without addressing these foundational challenges, the potential benefits of using AI to reduce improper payments may not be fully realized.

Technology and Tools to Keep Up with Adversaries

An important step in combatting improper payments involves limiting initial access to systems by adversaries. Whether the result of account take over, use of synthetic IDs, or other means, proper identity verification and validation is key in achieving this goal. Given advances in scams and the use of generative AI by bad actors to create deep fakes, the group discussed ways in which this is a significant challenge. Agencies need to focus on collaborative efforts to create more robust identity verification mechanisms. Those intent on receiving improper payments through fraud are increasingly sophisticated, using AI to create false identities, submit inaccurate applications, and redirect payments. This results in substantial financial losses and undermines public trust in government systems designed to support those in need.

Participants discussed the use of AI to create deep fakes and synthetic identities—which combine real and fabricated information to create entirely new identities or take over an innocent victim's identity. Once the tool of organized criminals, these technologies are becoming increasingly available to a wider population. One participant highlighted advances in generative video, image, audio, and text capabilities at a recent industry event that would make it difficult for traditional verification methods to distinguish between legitimate and fraudulent identities. Identities that appear legitimate on the surface can enable bad actors to bypass standard security measures, leading to improper payments and significant financial losses.

Balancing "Friction" with User Experience

While agencies should make it harder for adversaries to commit fraud, such actions should be tailored so as not to do so at the expense of poor customer experience for the vast majority of legitimate users. Most payments are "proper" and should not be slowed down. Consequently, agencies also face the challenge of how to accelerate legitimate payments safely, particularly in the context of government services where the mission is to provide timely and effective assistance to beneficiaries. This requires balancing secure login and authentication, policy design and execution, and the end user experience expectations set by experiences with banking and other consumer industries.

In addition, government policies and regulations, such as the Privacy Act addressed above, typically incentivize processes that take time to ensure a proper payment. This can present timeliness constraints in supporting those impacted by a natural disaster, where sending benefits quickly is paramount and can reduce time for fraudsters to prey on such events..

More broadly, overly stringent security measures can inadvertently create barriers that hinder access to services. For instance, complex identity verification processes may deter or delay eligible individuals from receiving benefits, especially those who are economically disadvantaged, elderly, or disabled. This can also erode public trust in government performance, as the very individuals who need support the most may find themselves entangled in bureaucracy.

The challenge is further compounded by the need to protect against increasingly sophisticated cyber threats and fraud attempts. False positives in distinguishing legitimate users from bad actors can lead to unnecessary scrutiny and delays. This not only frustrates users, but also places a significant burden on limited government resources.

DISCUSSION TOPIC TWO: OPPORTUNITIES FOR IMPROVEMENT

In the second part of the discussion, roundtable participants moved from discussing challenges to identifying strategies. Participants addressed actions to improve payment integrity in government. Three areas of focus emerged.

Focus Area 1: Collaboration

Collaboration across agencies and with industry will be key to a broad-based reduction in improper payments. Sharing research and development, technological advances, data and insights, alerts, and investigations—among agencies, oversight bodies, private sector partners, international organizations, and other stakeholders—can significantly enhance the identification and mitigation of improper payments. While this must be done carefully to avoid overreach, a secure and collaborative environment will allow agencies to develop more robust capabilities for reducing fraud and other improper payments. Agencies can scale the use of emerging technologies to share and analyze large datasets, identifying patterns and anomalies to surfacing bad actors.

Moreover, the exchange of information and best practices can help standardize procedures and policies across different entities, reducing inconsistencies that adversaries might exploit. For example, the financial services sector has developed innovative approaches to identity verification and fraud detection that could be adapted for use in government. This includes standardized governance and operating models with multiple lines of defense that agencies could leverage in detecting and responding to fraudulent activities. Additionally, international organizations can provide insights into global trends and emerging threats, allowing agencies to stay ahead. Finally, collaboration with oversight bodies and other stakeholders can enhance accountability and transparency in managing public funds and personal data.

A multifaceted approach to collaboration among agencies, industry experts, and legislative bodies can help all stakeholders work towards a common goal of reducing improper payments. Such collaboration can help government to update privacy and enforcement legislation, improve and safeguard data sharing capabilities, and invest in modern technologies.

In addition, collaboration with industry experts and technology providers can accelerate staying ahead of bad actors. Sharing knowledge, leading practices, and technological advancements can also help develop and apply more effective and resilient counter-fraud measures across more agencies and access points. These include sophistication in both security and access control as well as counter-fraud monitoring. By leveraging the expertise and resources of multiple stakeholders, governments can accelerate their ability to detect and prevent improper payments, thus ensuring that payments reach their intended recipients.

By fostering an environment that supports innovation while maintaining robust security measures, agencies can enhance user experience without compromising data and service integrity. This holistic approach can ensure that beneficiaries receive the timely and effective support they need, while also safeguarding against fraud and abuse—improving the efficiency and integrity of government programs and restoring public trust in their effectiveness.

Focus Area 2: Data and AI

It is not possible to discuss improper payments (especially fraud) and AI without addressing data and analytics. Ideally, the federal government would adopt a modern data strategy that standardizes common data structures, defines ubiquitous controls, and sets policies that balance payment integrity protection with privacy. This would include equipping federal programs with sufficient data capacity to better detect and prevent fraud and improper payments, particularly through the use of AI and machine learning. This can significantly enhance the accuracy and efficiency of identifying risky transactions.

> *(S)haring 'algorithms' that find and use data—versus sharing the data itself . . . addresses privacy concerns by not creating a single centralized data store, but rather a standardized approach to aggregating data from multiple data sources.*

In developing a modern data strategy, agencies should evaluate and revise their data practices, consistent with the digital techniques to ensure privacy and isolation. For example, AI can be used to perform many challenging tasks, such as analyzing vast datasets to detect patterns and anomalies, curate data, and create summaries for analysts and decision makers. This will not only improve productivity but will also call attention to potentially fraudulent activities that human analysts might overlook due to the sheer volume of transactions. By leveraging machine learning, government analysts can continuously improve detection capabilities by adopting new fraud tactics and reducing the incidence of improper payments. This proactive approach enables a shift from "pay and chase" to a more efficient pre-payment detection, identifying and stopping problems before funds are disbursed.

One intriguing idea brought forward by one of the agencies was the idea of sharing "algorithms" that find and use data—versus sharing the data itself. This addresses privacy concerns by not creating a single centralized data store, but rather a standardized approach to aggregating data from multiple data sources. This practice would enable one agency to benefit from advanced analytic techniques developed by another agency without compromising sensitive information. By using shared algorithms, agencies can maintain the confidentiality of their data while applying sophisticated fraud detection models developed from a broader dataset. This collaborative approach can foster a more unified and effective defense against improper payments across the federal government.

One roundtable participant discussed how their agency developed and deployed advanced AI algorithms to analyze large datasets and identify patterns that may indicate fraudulent activities. The algorithms identified approximately one million potentially fraudulent events, which prevented more than $10 billion in improper payments that would have otherwise been disbursed. By implementing predictive modeling and advanced algorithmic capabilities, agency staff prevented these improper payments, safeguarding taxpayer funds and enhancing the integrity of the tax system. Other agencies could consider a similar "moon shot" program to apply advanced AI to improve outcomes.

Integrating AI and machine learning into federal programs can streamline the process of verifying transactions and identifying improper payments in a rapid and secure way manner. Automated systems can handle routine tasks such as data entry and initial fraud screening, reducing the burden on human workers and minimizing the risk of human error. This will

improve the accuracy of payment processing and enable government analysts to focus on more complex cases that require detailed investigation. This will also enable an expedited path for most payments that are accurate and low risk.

In addition, advances in AI-enabled automation, including strategic use of generative AI, can reduce tasks that take agency staff hours or days to minutes or seconds, enabling agencies to confirm proper payments more quickly. Integrating AI and other advanced technologies to better verify identities, behaviors, and relationships can streamline processes and reduce the burden on users, while adding "friction" when warranted because of risks. For example, applying machine learning to reduce false positives in identity verification can significantly improve the accuracy and efficiency of the process. Additionally, adapting best practices from the private sector can help government to enhance both security and user experience. The financial services sector, for instance, has successfully implemented behavioral monitoring to complement identity verification, which could be adapted for government use.

Additional research and development into use of generative-AI and algorithmic processes, and sharing the findings and select data, can strengthen agencies' ability to collaborate to best address threats.

Focus Area 3: Technology

One key takeaway from the discussion pointed to the importance of layered defenses. While agencies must take steps to keep sophisticated adversaries out, monitoring is still required as no system is impenetrable. Behavior monitoring using advanced AI, combined with a broader view of data from various sources, can be used to spot changes in behavior indicative of an account take over, anomalies associated with fraud, or known behavior profiles associated with bad actors AI can enable agencies to analyze vast amounts of data in real-time and identify patterns and anomalies that present signals of abuse. The group discussed the possibility that AI can be used to cross-reference information from multiple sources, such as social media, government databases, or financial records, to verify the authenticity of a transaction or payment.

> *While agencies can apply their own policies to improve results, collaboration across government agencies and with industry experts can accelerate staying ahead of bad actors.*

An important topic for the group involved review of current policies for gaps or overlaps that can be exploited to limit the ability of agencies to share data. While agencies can apply their own policies to improve results, collaboration across government agencies and with industry experts can accelerate staying ahead of bad actors. Sharing knowledge, best practices, and technological advancements can also help agencies to develop and apply more effective and resilient counter-fraud measures across access points; such measures include sophistication in security and access control as well as counter fraud monitoring. By leveraging the expertise and resources of multiple stakeholders, government can accelerate capacity building to detect and prevent improper payments. This can help to ensure that payments reach their intended recipients while also maintaining the integrity of public programs.

Focus Area 4: Accountability and Transparency

A lack of accountability can result in a lack of focus on taking the necessary steps and making important investments to reduce the impact of improper payments. Instilling and rewarding (or penalizing) performance with respect to improper payments can help agencies focus on reducing the problem. Roundtable participants agreed that this will require changes outside of their control to implement, but felt it was important to quantify and recommend possible actions.

Agencies can use AI to assist in conducting regular audits and reporting on "scorecards" that tie performance metrics to payment accuracy. If properly developed, this could provide a structured and continuous evaluation of payment processes to bring a "continuous improvement" mindset to fraud prevention and payment integrity and execution.

While expanding regular audits will help in identifying discrepancies, errors, and potential fraud by thoroughly examining financial transactions and payment records, the use of AI in the audit process can improve both efficiency and effectiveness. This systematic review could help agencies detect and correct deviations from expected outcomes, thereby reducing the incidence of improper payments. By maintaining a consistent audit schedule, agencies can remain vigilant and responsive to emerging issues, promoting accurate payments that comply with relevant policies.

Utilizing scorecards that link performance metrics to payment accuracy introduces a quantifiable and transparent method for assessing the effectiveness of payment integrity efforts, and for highlighting areas for investment to shore up weaknesses. These scorecards can track key performance indicators (KPIs) such as error rates, the frequency of fraudulent activities, changes in fraudsters' access attempts, the volume of potentially improper payments, and the timeliness of payment verifications. By monitoring these and similar metrics, agencies can identify trends and patterns that may indicate underlying problems in the payment process. This data-driven approach allows for targeted interventions and improvements, ensuring that resources are allocated efficiently to areas most in need of attention. Moreover, scorecards provide a clear and objective measure of progress, helping to hold agencies accountable.

Furthermore, the integration of audits and performance scorecards can foster a culture of accountability and continuous improvement within agencies. When government officials and stakeholders know that their performance is regularly evaluated and tied to specific metrics, they have greater incentives to adopt best practices and maintain high standards of accuracy. This proactive stance not only helps in preventing improper payments but also enhances overall operational efficiency to safeguard taxpayer funds. By leveraging the insights gained from audits and scorecards, agencies can implement corrective actions, refine processes, and adopt new technologies to further strengthen payment integrity.

Focus Area 5: Skilled Workforce

The government workforce that works to reduce improper payments also presents a target for fraudsters. Continuous education for staff that manage payments will enable agencies to uphold payment integrity standards, while reducing improper payments. Skilled staff, augmented with AI tools and digital assistants, can stay informed on the latest policies, procedures, and technologies. This will help employees to identify and prevent errors, fraud, and other forms of improper payments. Training programs can cover a wide range of topics, including the use of AI and automation tools, data entry best practices, development and use of algorithms, and the importance of thorough verification processes.

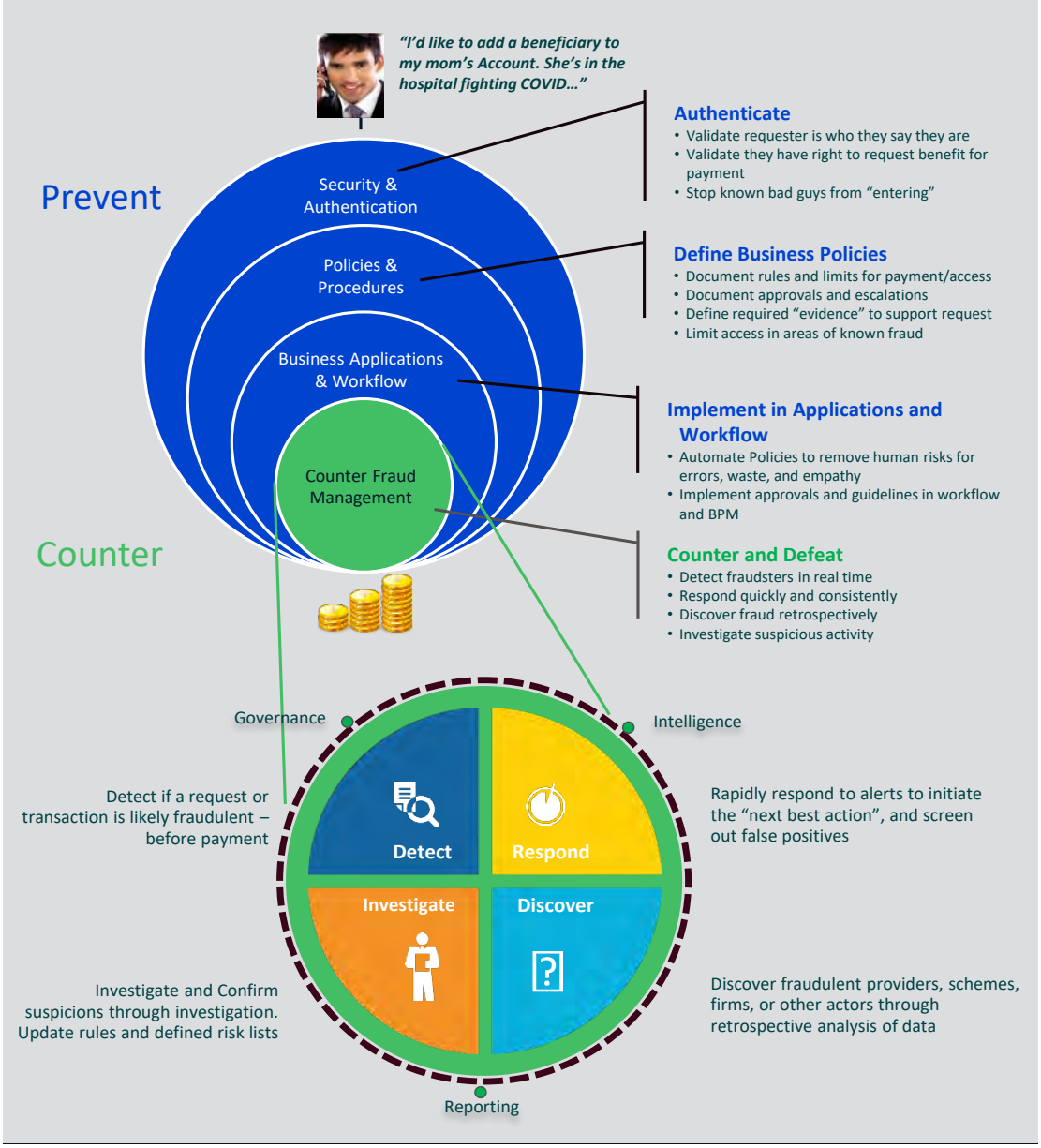
Such training can foster a culture of accountability and vigilance among payment management staff. When employees understand the significance of payment integrity and the potential consequences of improper payments, they are more likely to adhere to established protocols and suggest improvements. This heightened awareness can lead to more diligent monitoring and verification of payments, reducing the likelihood of errors and fraudulent activities slipping through the cracks. Additionally, ongoing training can help staff stay abreast of emerging threats and evolving fraud tactics, enabling them to respond swiftly and effectively to new challenges.

Finally, continuous education can facilitate better collaboration and communication within and across agencies. By standardizing training programs and sharing best practices, agencies can present a unified approach to payment integrity. This can lead to more efficient processes as staff from different agencies work together and share information. Enhanced collaboration can also help identify systemic issues and areas for improvement, leading to more effective strategies for preventing improper payments.

A Framework for Improvement

The observations, ideas, and actions from the roundtable can be mapped to create a “Counter Fraud Framework” that illustrates how each agency can break down actions to dramatically reduce improper payments. This framework arrays the roundtable ideas across a spectrum that starts with actions that could be implemented quickly, move to barriers that will take longer to break down, and describes the multiple layers of defense necessary to reduce improper payments. This can be used to inform efforts to modernize policies, regulations, laws, and operating models.

Figure 2: Framework to reduce the impact of improper payments



This framework, with key elements summarized in the above chart, addresses nine specific areas of focus to reduce the impact of improper payments:

1. **Secure Access:** As discussed, more sophisticated AI-powered identity management, security, and access control will be required to reduce the immediate threats of deep fakes created from increasingly accessible generative AI technologies. Strong, AI-infused access controls can identify risk and prevent improper payments before they happen.

2. **Policy Optimization:** Policies have been developed incrementally over decades—often attempting to implement multiple competing regulations without considering the evolving capabilities of modern technology—and have resulted in gaps, overlaps, and inefficiencies that can be exploited by adversaries. Payment integrity starts with re-imagined policies and procedures that align with innovative technologies and present-day threats. The private sector uses AI to review, align, and rewrite policies to help improve clarity and remove gaps and loopholes exploited by

fraudsters.

3. **Process Automation:** Automation can reduce risk of human error and collusion. Generative AI specifically can automate common tasks in support of a limited supply of specialists. By using automated processes to augment human efforts, government can speed up benefit processing, comply with competing policies in limited time periods, and better ensure that every payment is "proper." This has an added benefit of limiting bad actors' ability to exploit human errors in diverting or exploiting payment systems.

4. **Pre-Payment Detection:** Historically, agencies have employed "pay and chase" models so as not to hold up payments to citizens. In contrast, banks have used real-time fraud detection for more than 20 years at point of sale. By using AI-infused analytics and commercial techniques, agencies can begin moving from "pay and chase" to "pre-payment" checks that do not slow proper payments. This can send a strong message to fraudsters that their methods will no longer be effective.

5. **Response:** How agencies respond to transactional alerts is essential to reducing improper payments without slowing proper payments. AI and automation can allow for rapid responses to alerts, tips, and other events identifying potential fraud or other forms of interference with legitimate activity.

6. **Discovery:** "Pay and chase" still has merit as an element of a layered defense. Retrospective review of historical transaction data helps agencies to identify patterns, networks, and trends around sources of improper payments. This approach can provide insights that will improve the AI models used in detection. AI systems can also be used to identify trends and patterns and algorithms that can track evolving patterns.

7. **Investigation:** Agencies often face enforcement limitations and shortages of investigators, prosecutors, law enforcement to stop improper payments. The use of AI analytics and AI-enabled automation in investigations can confirm suspicions and rapidly identify the sources of fraud. Leads from response and discovery activities can be rapidly and accurately confirmed, providing information to support agency watch lists.

8. **Modern Data Strategy:** Building a data strategy may represent the greatest challenge. This spans the gamut, from using AI to better curate and pre-position data and revising laws and policies directing the use of advanced technology to allowing data and algorithm sharing in ways that ensures privacy protections. Generative AI can curate both structured and unstructured data, and advanced analytics can more rapidly identify the "signals" of fraud within the noise of vast data fields. Advances in encryption can improve the ability of agencies to share information securely while protecting identities. Effective data strategies can support actions that rapidly confirm proper payments, so that legitimate beneficiaries can receive benefits faster.

9. **Reporting and Accountability:** Agencies can create clear ownership and responsibility paths for improper payments. The private sector has a "bottom line" incentive. Similar motivations need to be instilled at all levels in public agencies. Moving improper payments from a "compliance" to a "results" posture will support agencies' efforts to follow through on making multiple improvements.

DISCUSSION TOPIC THREE: NEXT STEPS

While the roundtable recommended several strategic actions that government can continue to develop, each agency can also make their own improvements. Participants identified numerous steps that agencies can take to reduce loss, improve efficiency, and enhance customer experience.

> *AI can support government . . . [in] staying ahead of bad actors and improving the overall integrity of payment systems.*

Enhance Data Sharing Protocols: Agencies can work collaboratively to explore robust data-sharing protocols to ensure timely and accurate exchange of information. This involves creating standard procedures and systems that allow different government entities to share data seamlessly and securely. By doing so, agencies can improve their ability to enhance secure access by verifying identities, detecting fraud, and making informed decisions. Effective data-sharing protocols can also help to eliminate data silos within individual agencies, and promote a more integrated approach to managing and utilizing data. This integration is crucial for enhancing the overall efficiency and effectiveness of government operations, as it allows for real-time data exchange and better coordination among various departments.

Participants emphasized the importance of modernizing the Privacy Act of 1974. By developing agency-wide protocols and seeking a data/algorithm clearinghouse, agencies can share data consistently and accurately to improve identity verification and fraud detection. Participants also discussed developing and sharing algorithms in lieu of data to improve verification fraud detention protocols without breaching outdated data privacy rules until, and even after, modernized privacy policies are enacted.

Leverage Predictive Analytics: Agencies can develop predictive analytics by examining historical data, to uncover hidden trends and anomalies that suggest potential fraud and proactively address these risks before they result in improper payments. This approach not only helps in detecting fraud but also enhances the efficiency of payment processes, reducing the need for manual oversight and intervention. Predictive analytics can be integrated into existing systems to continuously monitor transactions and flag suspicious activities in real-time, thereby ensuring that funds are directed to their intended recipients.

Develop a Centralized Fraud Detection Hub: A cross-agency hub could enable agencies to share outcomes from fraudsters that may work across government. This centralized approach allows for the integration of advanced AI and machine learning technologies to analyze datasets in real-time, identifying patterns and anomalies indicative of fraud, waste, abuse, and errors before making payments. By leveraging predictive analytics, anomaly detection, and natural language processing, such a hub could proactively flag suspicious activities and prevent improper payments, thus enhancing the overall efficiency and integrity of the payment process. Additionally, a centralized hub would facilitate better data sharing and collaboration among agencies, reducing the silos that can impede effective fraud detection and response.

Invest in Advanced Fraud Detection Tools: Fraud is a specific type of improper payment that involves deception and misrepresentation, and is often difficult to spot. Agencies can invest in application monitoring and relationship tracking detection tools and technologies. These technologies can help government to analyze large datasets in real-time to identify patterns and anomalies indicative of fraud before payments are disbursed. By investing in modern IT infrastructure and AI-driven solutions, agencies can move from outdated "pay and chase" models to proactive pre-payment verification, with the goal of making only proper payments. This not only enhances the accuracy and efficiency of payment processing but also significantly reduces financial losses, thereby improving overall program solvency. These techniques have been proven within the private sector and can be adapted for government as well.

Utilize Machine Learning for Data Consistency: Agencies can employ machine learning to standardize and structure data across different systems. This helps prevent improper payments by ensuring consistency and accuracy in the data used for payment processing. Machine learning algorithms can help to identify and correct discrepancies, harmonize data formats, and integrate information from various sources, reducing the likelihood of errors. By creating a unified data structure, machine learning can facilitate better data analysis, enabling the detection of anomalies and patterns that may indicate fraudulent activities or errors. This proactive approach allows agencies to identify and address potential issues before payments are made.

Enhance Identity Verification and Monitoring: Strengthening identity verification processes and improving behavior monitoring can enable agencies to better detect an improper payment. This can significantly reduce improper payments by ensuring that only eligible and verified individuals receive payments. AI can enhance this process by helping agencies to analyze vast datasets to detect patterns and anomalies that may indicate fraud. For instance, AI can identify unusual behaviors or discrepancies in identity verification attempts, flagging them for further investigation before any payments are made. This preemptive approach would help to prevent improper payments by intercepting potential fraud at the verification stage.

Moreover, AI-powered identity verification and behavior monitoring can streamline the process, reducing the likelihood of human error and increasing efficiency. Traditional methods often involve manual checks, which can be time-consuming, prone to mistakes, and miss effective fraud schemes. By automating these processes, AI can help agencies to ensure that identity verification and behavior monitoring is consistent and accurate, minimizing the risk of overpayments, underpayments, or payments to ineligible recipients. Additionally, AI can support government to continuously learn and adapt given new fraud tactics, staying ahead of bad actors and improving the overall integrity of payment systems. This will be increasingly important as adversaries begin using generative AI to create deep fakes and synthetic IDs.

Conduct Regular Training and Awareness Programs: Agencies can provide regular training to staff on the latest fraud detection techniques and AI tools, enabling them to more effectively recognize patterns and anomalies that may indicate improper payments. This can enhance the proficiency and awareness of employees in identifying and mitigating problematic activities. This proactive approach allows for the early detection and prevention of fraudulent transactions before they are processed.

Moreover, regular training fosters a culture of vigilance and accountability within the agency. Employees with knowledge about the latest tools and techniques are more likely to maintain payment integrity. This heightened sense of responsibility can lead to more diligent verification processes, further minimizing the risk of errors and fraudulent activities.

Establish Clear Governance and Accountability: Agencies can designate an accountable senior official with has the authority to ensure that management, support and changes to improper payment verification and fraud prevention functions are done in a transparent fashion. Establishing a robust governance framework supports well-defined roles and responsibilities, crucial for maintaining oversight, enforcing anti-fraud measures, and tracking efforts to prevent improper payments. Additionally, clear governance structures facilitate better coordination and communication across programs, leading to more efficient and unified efforts.

Moreover, accountability mechanisms establish consequences for those who do not adhere to established protocols, which acts as a deterrent against negligence, collusion, and intentional fraud. When agencies have clear lines of responsibility and consistent reporting standards, it becomes easier to identify and address gaps in the system, and opportunities to fill gaps with the help of advanced technologies like AI.

Collaborate with Industry Experts: Agencies can partner with industry experts to stay updated on the latest fraud prevention technologies and practices, and to leverage advanced capabilities and innovative solutions. Cutting-edge commercial technologies, such as AI-driven analytics and machine learning models, can enhance the detection and prevention of improper payments. Collaboration can enable government to implement sophisticated fraud detection systems, optimize resource allocation, and improve overall payment integrity. Accountability and transparency protocols are especially important here to prevent unauthorized access or use of confidential public data and to reassure the public of those safeguards. By staying abreast of the latest advancements, agencies can proactively address emerging threats, streamline processes, and ensure that funds are disbursed accurately and efficiently, ultimately supporting program integrity and efficiency in the use of taxpayer dollars.

CONCLUSION

The roundtable identified numerous priorities and challenges shared across multiple agencies and recognized by stakeholders from Congress, academia, and business. Preventing improper payments can help ensure the solvency and sustainability of spending across key programs—limiting pressures to reducing benefits or increasing taxes.

AI provides a key technology to help agencies better understand and define the patterns and anomalies integral to identifying improper payments most effectively. Agencies can strengthen their use of AI for this purpose by leveraging data and collaboration, modernizing policies and regulations, and increasing accountability and transparency. This will require needed investment in technology and workforce skills. These and similar actions can help to improve government efficiency by reducing the impact of improper payments, which will promote program integrity and public trust.

Part 2—Detailed Roundtable Discussion Summary

DISCUSSION TOPIC ONE: CHALLENGES

Challenges identified in previous events and articles—including bad actors and the technology and tools to keep up with them, "identity protection and customer experience, siloed agencies and systems, and outdated laws"[5]—continue to plague payment integrity. In this discussion, participants identified additional significant challenges, lessons learned, and opportunities to move forward.

1. **Capacity limitations:** "Anti-fraud practices are where cyber practices were 20 years ago," remarked one roundtable participant. Capacity in all its forms—equipment and hardware, administrative structures and trained personnel, and internal controls are all means of support to bring internal systems and policies into the 21st century. Most challenges have their foundations in capacity restraints. One participant commented, "I think Congress gets confused. They think the Inspectors General [IGs] are the starting point for detection of fraud. . . . We need funding at the administrative level . . . to look for fraud and identity." In addition, from hardware and software to social media and cyber detection tools, agencies are vastly under-equipped when it comes to keeping up with new media for data collection and verification, and sophisticated techniques to exploit weaknesses identify security.

> *We're seeing a dedication of the bad actors to truly assume other identities. Their commitment to this identity is fully encasing. They do all the social media posting, data mining, and data analysis to protect identities better than any I've seen. They're so good, in fact, that thelogin.gov team has been hiring them.*

2. **Identity integrity:** Identity verification and confirmation continue to challenge departments and agencies. False positives, identifying and deterring bad actors, distinguishing legitimate bot traffic from predator bots, and siloed data continue to stymie efforts to determine identification validity.
3. **Antiquated laws and ineffective controls:** The legal framework that governs data sharing, within agencies and across agencies was developed in the 1970s—the Privacy Act of 1974, the guideline for determining the limits of data sharing, is now more than 50 years old. This framework is used for each occurrence. "Every single time it is like running a marathon to share a new data set," noted one roundtable participant." This inhibits agencies' ability to share information making identify verification and fraud detection very difficult. This also slows the development of advanced algorithms for risk assessment and prevention, and creates two other challenges.
    - **Lack of enforcement:** Ineffective laws and limited resources necessary to enforce and prosecute bad actors when they are identified. Current, outdated laws never anticipated the methods used for identity validation or the methods used by fraudsters for identity theft. As one participant noted, "For IGs and prosecutors, it's hard to put in the time chasing and prosecuting unless it's a huge ring."

5. Chenok & Dommel. Modernizing Government Payment Systems to Improve Efficiency and Effectiveness.

- **Internal controls** are difficult to implement in emergencies, to make sure payments are made to all entitled recipients. For example: (W)ho does the Chief Anti-Fraud Officer report to? What powers do they have? How do they enforce better identity? Moreover, there is no Chief Anti-Fraud or Payment Integrity Officer in many federal agencies—and where they do exist, they are undefended and understaffed. Finally, absent a law, policy, or regulation requiring such focus, there is often a lack of motivation or leader assigned to focus on stopping fraud and measuring or rewarding results.

> *We need a central clearinghouse, at least for fraud, to share information with other agencies recognize when we see [it]. . . . It's about protecting citizens from [identity] fraud and being able to share key indicators. So other agencies can be protected as well. . . . We need to balance the security side with the usefulness of the process being employed and data used.*

4. **Data sharing:** Stove-piped programs in and across agencies can hinder real-time data exchange. Each agency has its own variable data structure, challenging their ability to provide legitimate translations to data requests. For example, agencies may get yes/no answers to questions like date of birth, address, or queries for information that does not enter a common data repository. Also, identifying and correcting for bias (conscious and unconscious) can be arduous. Arriving at single sources of truth in that data is difficult.
5. **Other challenges:**
    - **The life cycle of grants management** produces reams of documents and intense workflow management that is onerous for agencies, partners, and recipients. This also applies to benefits and claims processing, and other financial processes.
    - **The use of AI is a key issue.** The federal government needs to acknowledge that AI's use can be more seriously supported and more extensively used for analytics and automation. This will improve identification and payment security and detect and deter payment and cyber fraud before it happens

DISCUSSION TOPIC TWO: LESSONS LEARNED

Participants addressed lessons learned in multiple areas.

1. **Data and algorithms:** As one participant noted, checking identities produces "gazillions of false positives. . . . Each one of those drives you to conduct enhanced due diligence, which is extremely expensive." Applying machine learning to reduce false positives significantly improved the integrity of the real positives. In addition, sharing algorithms instead of databases can reduce data privacy issues.

   Lessons Learned: AI can create an algorithm that travels. Then the algorithm, rather than the data, can potentially be shared with another agencies, reducing privacy challenges.

   - Algorithms can help agencies learn from other agencies, as evidenced by successes in the private sector. However, one participant noted that this also generates "issues associated with ensuring against bias and having objective third parties who are able to do that."
   - Challenges in applying algorithms against widely "variant data sets," particularly as agencies have wildly different structures to their data.

2. **Integration of social and news media:** One agency uses AI to scan online articles and news stories to build more robust datasets and algorithms.

   Lessons learned: There is a need for protocols and a central clearinghouse. There must be a mechanism to help create data and algorithmic consistency. Application of AI across data sets, and establishing enterprisewide protocols, could eliminate the need for storing or sharing the underlying data at each source. This would eliminate an agency's need to always play "catch-up."

3. **Organization driven change through collaboration:** Collaboration enables more support and knowledge attained with less resources expended.

   Lessons learned: The Council on Federal Financial Assistance (COFFA), a collaboration between CIOs and CFOs across agencies, provides federal officials with basic knowledge training on grants and cooperative agreements. COFFA is based on a peer-to-peer governance structure that uses bottom-up and top-down information. Collaboration like that done through COFFA can address several challenges for agencies: (1) quickly being outpaced by need; (2) difficulty in partitioning time; (3) no assembly of different agencies to advise; (4) need to encourage government to invest to be more effective; and (5) need to establish protocols that don't overload the organization.

4. **More effective ways to identify and eliminate active and inactive colluders:** Agencies can learn from cyber detection practices as they evolve and expand to embrace alternative technologies. Leaders can examine cyber best practices to identify those that may aid in identity validation, and may be enhanced though the application of AI. Updated equipment, systems, and enforcement, as with cyber detection, may also be required.

Lesson learned: Cyber detection and deterrent processes may be applicable to develop AI identity and payment security protocols.

5. **Public/private collaboration:** The financial services sector has used AI for some time to balance user access and security and identity verification to comply with their "know your customer" mandate, and to expedite customer interactions. They developed innovative approaches to addressing the customer onboarding process that could be applicable to federal agencies' identity verification needs. However, banks found that identity verification alone was not enough; their solution was to add behavioral monitoring to create digital verification, which casts a broader net for identity confirmation and fraud identification. When a customer accesses their account, any change in behavioral patterns will alert the bank, for example. This enables real time detection, allowing the bank to determine validity, and intercept future payments as needed.

   Lesson learned: This may be challenging to implement in public agencies, but theories and implementation of behavior observation, combined with other AI techniques for identity verification and other relevant actions, could inform federal AI development efforts.

   - **Leveraging industry partnerships.** Combining industry knowledge, innovation, and experience to build more effective and efficient verification processes can bring minds and investments together. For example, how might social media, or e-commerce tools be used to strengthen federal processes? Shared services might adapt work in specialized industries, such as financial services and technology, to build on AI-driven fraud detection and prevention and ways to react to anomalies. Agencies can also work with industry on addressing cyber fraud, and solicitation of industry for models that could be applied when cyber units support protecting improper payments data.

     Lesson learned: In order to leverage industry capability, agencies should address the challenges applying corporate solutions to government practices, including orientation (profit driven vs. public service driven), funding, technology and process compatibility, ownership and privacy of data collected, and algorithms developed/used.

   - **Leveraging internal partnerships.** Agencies share concerns and explore ways that AI can be used in a cross-government fashion. Exploration of self-certification issues, perhaps using IRS and bank practices examples, offer opportunities to react more effectively to anomalous transactions.

     Lesson learned: Agencies should address any reticence to engage AI due to the lack of consistency in definitions and evolving maturity of the technology.

6. **Investment:** Some agencies have proposed and driven investment for anti-fraud efforts. Other agencies have not due to funding constraints.

   Lessons learned: Scarce funding limits the extent to which agencies can explore and implement AI for payment security. Alternative funding ideas include partnering with industry and collaborating with other agencies (see above). However, investing in AI and supporting technologies will show cost savings due to increased efficiencies.

DISCUSSION TOPIC THREE: NEXT STEPS

In this last discussion, participants identified areas and techniques where AI analytics and automation can reduce loss, improve efficiency, and enhance customer experience. Several short-term, mid-range, and long-term priorities and actions were identified, as well as overarching issues that influence forward movements.

Immediate and Intermediate Steps

1. **Adapt best practices and identify resources needed for implementation.**
    - *Cyber best practices.* Implement cyber security best practices, especially for identity security, thresholds for data sharing, and identifying risky actors.
    - *Data management.* Develop enterprise-level rules to determine the balance between the right amount of data sharing and minimizing privacy and other risks.
        - Build profiles based on confirmed bad actors. Then use that profile to look for anomalies that follow the same pattern. Integrate capabilities for behavior observation.
        - Use AI to create "vulnerability" indexes that can be applied. Higher levels of security and due diligence can be applied to the more vulnerable.
        - Pilot generative AI to ask questions and assess risks and preempt fraud, and develop algorithms to manage these assessments.
        - Build out governmentwide standards and services such as "do not pay" and "account verification" to mitigate improper payments.
        - Use metrics to determine extent of successes.

2. **Modernize existing systems.** To the extent that resources are available or may be reprioritized or requested, use them to consolidate and upgrade systems, operations, and administration of identity security. Retire and replace legacy systems, create data mining mainframe environments, and institute sharing and examining data to develop viable algorithms that can be upgraded as needed.

3. **Push the envelope when it comes to efficiency and effectiveness.**
    - Continue to expand efforts to reduce improper payments through identity fraud. Assign ownership and accountability and measure and hold accountable for results.
    - Introduce and integrate AI in areas such as reading and interpreting contracts, policies, grants, and other documents to highlight gaps and inconsistencies. Streamlining policies can reduce improper payments by lessening the complexity required to confirm a payment is proper. For grants management specifically, use modern AI to assess risk and reduce document and reporting requirements; aid in the award verification and selection processes; maintain subsequent tracking, oversight, analysis, and reporting of awards; and generate historical agency and enterprise comparative data. This could be done by developing and implementing an algorithm that would compare awards, payments, and verification efforts to existing laws, internal policies, and interpretations.

- Use AI to identify additional pathways to reduce improper payments, such as system improvements, new approaches to identity protection and fraud prevention, and ways to monitor distribution of goods and services.
- Continue to learn/share new applications and challenges with industry and agency partners.

4. **Update legislation and policies.** Update the Privacy Act and other relevant legislation and polices that are outdated, often by decades. Current privacy laws make data sharing for fraud detection and enforcement more difficult, and inhibit agencies' ability to prevent improper payments, detect bad actors, and share information with other agencies. This also slows the development of advanced algorithms for risk assessment and prevention.
5. **Create an independent committee focused on payment integrity.** Using COFFA as a model, create an independent coalition to coordinate across silos, with identified roles and goals, to develop standards for identity and payment security and the integration of AI into relevant processes. This entity could identify support needed (including funding, systems, personnel and technologies), establish enterprisewide best practices, develop structures for creating and sharing algorithms, and liaison with congressional and other stakeholders on capacity building, fiscal support, bill and rule drafting, and administration and leadership.

Long-Term Steps

1. **Work with leaders from government and industry to drive awareness and support for AI as a key government asset.** Recent cyberattacks illustrate the importance of AI and cyber fluency. Increasingly sophisticated global technologies illustrate the importance of staying ahead of adversaries for reducing improper payments due to cyber breaches and identity fraud. Efficiencies from AI can be especially important when reducing government spending is a top priority.

   Such collaboration can support ongoing, enterprisewide initiatives that include:

   - Meeting industry-standard levels of continuing investment
   - Flexibility in acquisition
   - Educated and informed leadership
   - Sophisticated technologies to complement and build out missions, leveraging of social media
   - Enhanced government data sites such as USA Spending and Login.gov
   - An enforcement clearinghouse, perhaps integrated with state and local government efforts

2. **Continually engage industry experts.** Explore ideas and options for large-scale leveraged partnerships that include building systems, implementing state-of-the-art technologies, mentoring personnel, designing AI-based algorithms, and performing updates to remain current with sophisticated cyber and identity fraud practices. This can help government address challenges that will include system modernization, AI and data ownership, and data and algorithm privacy and access.

APPENDIX

ROUNDTABLE ORGANIZATION LIST

- Arnold Ventures
- Ceenic Solutions
- Committee on House Oversight and Accountability
- Department of Agriculture
- Department of Health and Human Services
- Department of Housing and Urban Development
- Department of the Treasury
- House Committee on Oversight and Reform
- Internal Revenue Service
- National Academy of Public Administration
- Office of Personnel Management
- PNC
- Program Integrity Alliance
- Social Security Administration
- The Center for Organizational Excellence
- West Virginia University

ABOUT THE AUTHORS

Richard Hoehne
Georgia State University

W: linkedin.com/in/richardhoehne

Richard (Rick) Hoehne is an Advisory Board Member with the Maurice R. Greenberg School of Risk Science at Georgia State University with expertise in the area risk, fraud, and financial crime.

The Maurice R. Greenberg School of Risk Science's Advisory Board comprises business leaders who possess expertise in risk management, actuarial science, and insurance as well as a deep commitment to M.R. Greenberg School's mission.

Following a 27-year career in the private sector, Rick has shifted his attention to research in the area of risk, fraud, and financial crime, with an emphasis on the unique challenges faced by federal and public organizations. Rick founded and launched a Risk, Fraud, and Financial Crime Center of Competency where he spent the past 15 years developing solutions and working with public and private organizations around the world to mitigate the risk of fraud, money laundering, and other criminal activities.

Dr. Karen Kunz
Associate Professor Emerita
West Virginia University
Morgantown, WV 26505-6322

W: https://publicadmin.wvu.edu/faculty-and-staff/public-administration-directory/karen-kunz-dpa
E: Karen.Kunz@mail.wvu.edu

Dr. Karen Kunz is an Associate Professor Emerita at West Virginia University. In addition to teaching graduate courses in public finance and fiscal policy, Dr. Kunz has coauthored two books, *When the Levees Break: Revisioning Securities Regulation* (2016), and *The Cost of Congress* (2021, www.thecostofcongress.com), which was supported by a Congressional Research Grant from the Dirksen Center.

She has collaborated on numerous articles on varying topics including public leadership, federal fiscal policies and practices, and political philosophy, and received an award from Emerald Publishers for Outstanding Author Contribution for the book chapter Unsettling the Memes of Neoliberal Capitalism through Administrative Pragmatism.

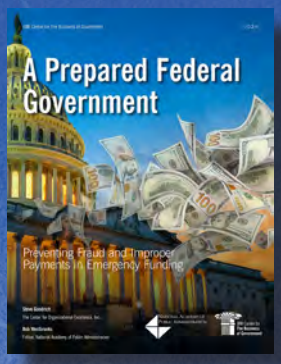
Prior to joining academia, Dr. Kunz was employed in the financial services industry. She developed and operated a consulting firm in Los Angeles that provided administrative, audit, and compliance services to multinational and boutique firms within the sector.

Dr. Kunz is an active board member and officer for two organizations, including the American Association of Budget & Program Analysts (AAABPA) and the West Virginia Food and Farm Coalition. In addition, she is a U.S. Army Veteran.

Recent Reports from the IBM Center for The Business of Government

Digital Modernization for Government: An Implementation Framework

by Dr. Gregory S. Dawson, Dr. James S. Denford, Kevin C. Desouza and Marc E. Barda Picavet

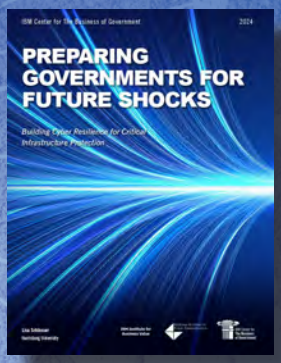


A Prepared Federal Government: Preventing Fraud and Improper Payments in Emergency Funding

by Steve Goodrich and Bob Westbrooks

Resilience in action: Crisis leadership through innovation, collaboration, and human-centered solutions

by Challenge Grant Case Study Recipients

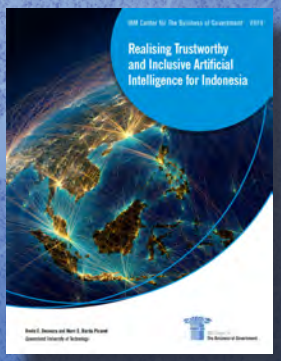


Preparing Governments for Future Shocks

by Lisa Schlosser

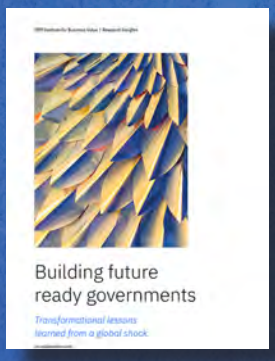
Navigating Generative AI in Government

by Alex Richter



Realising Trustworthy and Inclusive Artificial Intelligence for Indonesia

by Kevin C. Desouza and Marc E. Barda Picavet



Building future ready governments—Transformational lessons learned from a global shock

by Cristina Caballe Fuguet, Kee Won Song and David Zaharchuk

Building On Regulatory Foundations and Bridging to the Future

by Dan Chenok and Susan Dudley

For a full listing of our reports, visit businessofgovernment.org/reports

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Consulting

With consultants and professional staff in more than 160 countries globally, IBM Consulting is the world's largest consulting services organization. IBM Consulting provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, D.C. 20005
(202) 551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:

IBM Center for The Business of Government