DOCUMENT NUMBER MTR160040
MITRE TECHNICAL REPORT

MITRE

GOVERNMENT-WIDE PAYMENT INTEGRITY: NEW APPROACHES AND SOLUTIONS NEEDED

McLean, VA

February 2016

Acknowledgments

The MITRE Corporation – a private, not-for-profit organization – operates federally funded research and development centers (FFRDCs), unique organizations sponsored by government agencies under the Federal Acquisition Regulation to assist with research and development, study and analysis, and / or systems engineering and integration. MITRE operates seven FFRDCs sponsored by the federal government. These are:

- National Security Engineering Center sponsored by the Department of Defense,
- Center for Advanced Aviation System Development sponsored by the Federal Aviation Administration,
- Center for Enterprise Modernization sponsored by the Department of the Treasury, Internal Revenue Service, and co-sponsored by the Department of Veterans Affairs,
- CMS Alliance to Modernize Healthcare sponsored by the Centers for Medicare & Medicaid Services,
- The Homeland Security Systems Engineering and Development Institute sponsored by the Department of Homeland Security,
- Judiciary Engineering and Modernization Center sponsored by the Administrative Office of the U.S. Courts, and
- National Cybersecurity Federally Funded Research and Development Center sponsored by the National Institute of Standards and Technology.

MITRE also maintains a broad, independent research program, designed to explore emerging issues and potential solutions to benefit our government sponsors, industry and the public.

This study was conducted as an independent, internally funded study. MITRE interviewed representatives of a number of federal agencies, federal oversight and accountability organizations, industry, academics, professional organizations, non-profit organizations, and a foreign government. A complete list is shown in Appendix A of the report. MITRE wishes to thank all of these organizations for their time and contributions to the study.

MITRE Study Team

Dr. Shaun Brady
Gary Ingber
Gordon Milbourn
Jon Stehle

MITRE Payment Integrity Advisory Group

Paul Bielski
Andy Buckler
Robert Case
Mark Crain
Bahaa Fam
Jasmine Faubert
Dr. Arnold Greenland
Alanna Lavelle
Kevin Lewis
Dennis Sawyer
Karen See

Abstract

According to the Office of Management and Budget, the federal government annually makes more than $3 trillion in payments of all kinds, the great majority of which are proper. However, in fiscal year 2014, federal agencies estimated that they made nearly $125 billion in improper payments, representing the equivalent of the sixth largest agency. The amount of reported improper payments more than doubled over the last decade, but these estimates do not include all programs.

The MITRE Corporation, a not-for-profit corporation that operates federally funded research and development centers on behalf of federal government sponsors, conducted this independent, internally funded study of federal Payment Integrity[1] in conjunction with its charter to help address significant government-wide problems. The study discusses the following issues.

- Trends involving such things as economic pressures, healthcare issues, cyber-based crime, and the behavior of fraudsters that could continue to impact Payment Integrity.
- How government agencies address Payment Integrity challenges, present improper payment information to stakeholders, focus on agency actions as opposed to actions of federal payment applicants, and assess risk, and the impact of these approaches on corrective actions.
- Primary areas of vulnerability and risk that contribute to improper payments.
- Obstacles that contribute to improper payments by hindering agencies' ability to prevent or identify them.

This study describes the impact of these issues and recommends 15 actions for broader, more cross-government approaches and transformational solutions to enhance Payment Integrity across the federal landscape.

[1] Payment Integrity refers to improper payments and the people, processes, and technology that are meant to ensure that the payments are actually proper.

Executive Summary

According to the Office of Management and Budget (OMB), the federal government annually makes more than $3 trillion in payments of all kinds, the great majority of which are proper – made to the right person or entity, for the right reason, at the right time, in the right amount. However, in fiscal year (FY) 2014, federal agencies estimated that they made nearly $125 billion in improper payments (4.0 percent of all payments). This represents the equivalent of the net cost of the sixth largest federal agency, but is only for 124 of the hundreds of federal programs. The overall amount of improper payments more than doubled over the last decade, producing a level of improper payments that is unaffordable and adding to the current difficult economic picture.

Improper payments contribute to public concerns about the effectiveness of the government's stewardship over taxpayer dollars, and Congress and the Executive Branch have taken notice. Since 2002, Congress has enacted at least five statutes addressing aspects of fraud and other improper payments, and a number of Executive Orders, presidential memoranda, and OMB memoranda and guidance have been issued. Extensive efforts have been made in recent years to estimate and report on improper payments in individual federal programs, yet important questions remain about the nature of the improper payments themselves, especially:

- What are the ***real numbers*** – the dollars, and the rate?
- What is a ***realistic, cost-effective level*** to which improper payments can be reduced? What level of "residual risk" – which could vary by program, agency, or domain – is reasonable to accept?

Leadership of The MITRE Corporation (MITRE), a not-for-profit organization that operates federally funded research and development centers on behalf of federal government sponsors, recognizes the impact that the overall federal Payment Integrity[2] situation has on government effectiveness and public confidence. Given the public interest nature of this challenge, MITRE conducted this independent, internally funded study to assess the underlying systemic factors that enable fraud and other improper payments and to explore government-wide solutions to improve Payment Integrity.

We acknowledge the considerable efforts already in place at OMB and across federal agencies focused on identifying, reporting and mitigating improper payments. The objective of this study is to provide useful input and new insights to those efforts by addressing these key questions:

- What trends may be coming that could adversely impact the rate or the total dollars of improper payments?
- What are the root causes of the current improper payments?
- What obstacles must be addressed to make greater progress toward solutions?
- How can the federal government attack the problem in more effective, proactive ways?

Based on the nature and scope of federal Payment Integrity challenges and the key questions to be addressed, we performed a qualitative analysis using interviews, observations, and informed

[2] Payment Integrity refers to improper payments and the people, processes, and technology that are meant to ensure that the payments are actually proper.

interpretation. The study's conclusions revolve primarily around how agencies address Payment Integrity, not the quantitative results that they report; consequently, the study does not cite extensive numbers – either in describing the present or predicting the future. The study should be viewed as the starting point for further investigation; additional analyses – both qualitative and quantitative – on a number of Payment Integrity issues would be valuable next steps.

Numerous trends suggest that Payment Integrity problems could worsen

A number of trends could adversely impact the dollars and / or the rate of improper payments in federal programs.

- Economic pressures from continuing growth in the national debt and federal expenditures, along with declining labor force participation, will likely continue to increase the number of people participating in means-tested benefits programs.
- Healthcare issues and demographic changes are expected to continue straining existing healthcare and age-related means-tested benefits programs. Healthcare fraud, in particular, has been increasing in recent years.
- Extreme events can demand increased provision of services and benefits (e.g., in responding to and recovering from damaging hurricanes). These events have been increasing in recent years, and the need to respond more quickly than in traditional benefits programs makes them more susceptible to fraud, waste, and abuse.
- Technology is helpful in preventing and detecting improper payments, with numerous commercial tools and access to an increasing array of available data. But it introduces new vulnerabilities that outside agents can and do use to undermine Payment Integrity, and financial crime today is increasingly technology-driven.
- Cyber-based crime is expected to continue increasing due to low cost of entry and ease of execution, and government programs are especially vulnerable. It is much easier and cheaper for a cybercriminal to launch an attack than it is for an agency to defend against one.
- Statutes are increasingly impacting the relationships between government programs, often expanding the interrelationship / duplication / overlapping of programs and creating complexity in fighting improper payments.
- Fraudsters' behavior is increasingly sophisticated, changing, and ubiquitous. The increasing boldness of fraudsters and the globalization of fraud and related financial crimes are expected to continue to challenge organizations.

Each of these trends is already occurring to some degree, and other, currently unanticipated, trends may surface. That said, there is the potential that the already significant government improper payments problem could worsen because of these trends, calling for proactive consideration of these potential events and thoughtful attention to what should be done to mitigate their impact.

How the federal government approaches Payment Integrity contributes to sub-optimal corrective actions

The study identified a number of concerns with the way the federal government approaches Payment Integrity that have a detrimental effect on solving the problems. First, how the federal government currently categorizes and reports improper payments can confuse stakeholders. Reported improper payments include:

- Both actual and potential improper payments, but many stakeholders seem to "hear" them as all actual
- Both underpayments and overpayments, but many stakeholders seem to "hear" them as all overpayments
- Both fraud and errors, but many stakeholders seem to "hear" them as all fraud

The importance of Payment Integrity to federal managers and employees is driven, in large part, by the message sent by top leadership. An organization needs to have a philosophy that fraud, waste, and abuse is considered to be a problem; "tone at the top" is critical, with top leadership "owning the problem." However, this is not always the case across agencies. In some agencies Payment Integrity is viewed as a Chief Financial Officer issue, while in others multiple executives are responsible for different aspects like reporting, operations and execution management. Top leadership emphasis across agency components is critical; for example, at the Social Security Administration (SSA) a senior level Improper Payments Oversight Board works across the agency to solve improper payments problems and shape Payment Integrity strategies.

It is critical to understand the "true" root cause of a problem in order to formulate effective corrective actions. Identifying the true root cause can be difficult, and agencies do not always appear to dig deep to find the true root causes of their improper payments, often settling for apparent root causes (also called "causal factors"). Further, agencies rarely recognize fraud as a root cause of improper payments.

In identifying root causes and formulating corrective actions, agencies seem to most often focus on "government" errors but not "applicant" errors or fraud, leading to many "catch the agency error" vs. "prevent the applicant error / deter the applicant fraud" corrective actions. However, it is generally less expensive and risky to prevent applicant errors and deter applicant fraud than to catch errors before payment. This approach can be called "left of check" (see Figure ES-1), i.e., the further to the "left" of (before) the issuance of a payment in the overall process that the payment is stopped, the less expensive and risky to the organization. The worst case is to make improper payments and then attempt to recover them – often termed "pay & chase" – which Government Accountability Office (GAO) officials called a fundamentally flawed approach.

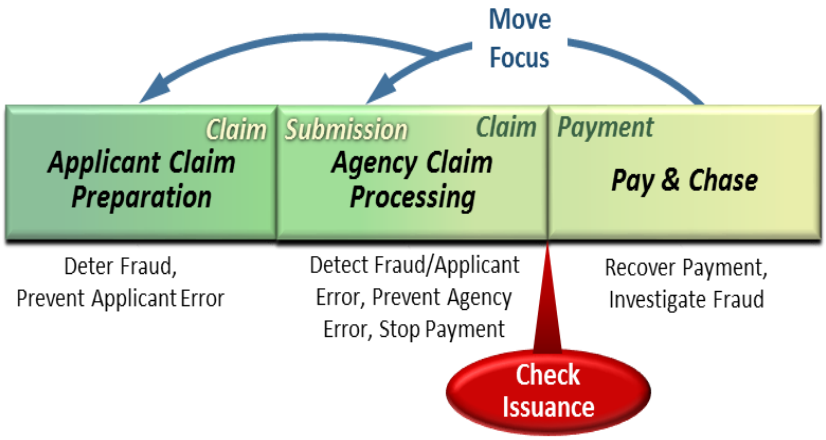


Figure ES-1. "Left of Check" vs. "Pay & Chase"

Improper payments reporting categories are a mix of actual root causes and internal control problems. This comingling of root causes and internal control problems may be leading agencies to corrective actions that do not resolve the real problems that created the improper payments and may hinder the identification of systemic root causes and the development of cross-government strategies to address them.

Further, it is usually easier for an organization to solve problems that are under its direct control than those that are not. In the case of improper payments, key aspects of many programs are outside agencies' control, making it more difficult to solve the Payment Integrity problems. For example:

- It is difficult for agencies to proactively impact the behavior of applicants in order to prevent errors or deter fraud.
- While agencies can control their own processing of applications and payments, they can only guide / require and oversee other entities (e.g., states, grantees) that might have key responsibilities in the process.

In addition, agency officials often described a "tension" between ensuring that payments are proper and getting them into the hands of the individuals who need them at the time they are needed. However, as GAO stated in its July 2015 document, *A Framework for Managing Fraud Risks in Federal Programs*, "the purpose of proactively managing fraud risks is to facilitate, not hinder, the program's mission and strategic goals by ensuring that taxpayer dollars and government services serve their intended purpose."[3]

Two emerging concepts in financial crimes – "commonalities" and "convergence" – impact federal improper payments. "Commonalities" refers to the fact that all financial criminals need, for example, to evade taxes and to launder money. Because financial crimes have commonalities, "convergence" refers to the need to bring agencies overseeing the various offenses – the Internal Revenue Service (IRS) with tax fraud, the Financial Crimes Enforcement Network with money laundering, etc. – together with new, more holistic approaches in order to fully address the problem.

[3] A Framework for Managing Fraud Risks in Federal Programs (GAO-15-593SP, July 2015)

Finally, some agency and accountability officials raised questions about whether the Improper Payments Elimination and Recovery Act (IPERA) of 2010 (P.L. 111-204) risk assessment process provides for addressing all programs that it should, and whether it focuses sufficiently on fraud; others expressed confusion about how to apply OMB's existing guidance and overall approach. Risk assessments should be conducted at a business unit or program level in such a way that the results can be aggregated with those of other, similar units or programs, up to and including aggregation at the enterprise level. In the federal government, some issues are common across domains or even across the entire government, such that the government itself could be viewed as "the enterprise" for aggregation and assessment purposes. However, the "silo" mentality often found in agencies can make aggregating the risk assessment results a challenge. Finally, in considering risks, having common risk classifications – a taxonomy – is important for clear communication and understanding, and for effective mitigation.

Recommendations: Federal approach to Payment Integrity

Given the nature of many of the issues identified by the study, broader, more cross-government approaches and transformational solutions are needed. With that in mind, we make the following recommendations.

1. Designate a federal executive to chair a leadership group comprised of agency principals to define and oversee a Payment Integrity strategy that addresses government-wide and, as needed, domain-wide issues, and to demonstrate a strong "tone at the top."
2. Clarify root cause reporting categories in OMB Circular A-123, Appendix C, in light of statutory wording defining "improper payment."
3. Focus more on preventing errors and deterring fraud than has historically been the case.
4. Assess existing metrics to determine whether they can better measure the effectiveness of individual agency corrective actions addressing root causes.
5. Develop a comprehensive and ongoing risk management framework addressing Payment Integrity risks, in particular fraud, based on threat analysis to help agencies better understand their vulnerabilities and better define defenses.

Preventing and detecting certain improper payments is a significant cross-government challenge

The impacts of both identity and eligibility on Payment Integrity can be significant. The challenges of verifying identity and eligibility cut across many programs and are often similar in their nature from one agency to the next. However, there is currently no capability across government for verifying applicants' identities or eligibility.

- In recent years important segments of the private sector have instituted preventive controls that feature a customer identification and due diligence program, often called Know Your Customer (KYC), to help organizations positively identify potential customers and key information about them before conducting financial business with them.

- Determining eligibility is complicated by a number of factors, including definitional issues in legislation that can be confusing, legislative requirements for such things as the timing of payments that can hinder agencies' ability to verify eligibility before making the payments, and program design issues (whether legislatively mandated or agency-established) that position agencies to rely heavily on self-reporting by benefit recipients.

IDENTITY AND ELIGIBILITY

Given the government-wide nature of the challenges presented by identity and eligibility issues, one of MITRE's most important recommendations (#9 below) is to identify and pilot-test alternatives for making identity and eligibility determination processes more rigorous, data driven, and cost-effective.

A significant concern is often the availability of the data needed to verify eligibility. In some cases data may not exist to allow agencies to independently verify eligibility. In others, data may be available, but agencies are prohibited from using it or do not have matching agreements in place to take advantage of it. Finally, data may exist and can be matched, but there may be problems with the data itself, such as poor quality.

Some agencies have worked to share data to help with eligibility determination. The Centers for Medicare & Medicaid Services (CMS), for example, has established a federal data hub to allow itself and the states to access a variety of data sources from the IRS, the Department of Defense TriCare, SSA and the Office of Personnel Management to help with determining eligibility.

Further, data analytics are an integral part of control activities to prevent and detect improper payments, and a wide array of commercial tools and methodologies exist to help fight improper payments. Federal agencies have undertaken a number of significant analytic efforts to reduce improper payments, such as CMS' Fraud Prevention System and the Department of Labor's Unemployment Insurance Integrity Center of Excellence. However, it is important to acknowledge what industry experts emphasized – that while analytics are critical to keeping up with ever-changing fraud schemes, the real key to achieving success with analytics is not so much the specific approach or tool used, but rather the ***data***, in particular determining which features in the data to leverage. Further, having ***what*** data is needed (including sharing data among agencies and having access to all needed commercial and open source data sets), ***when*** it is needed, at the level of ***quality*** that is needed, are all critical for successful analytics, but are often major challenges for agencies.

A number of additional challenges are present in the Payment Integrity analytics environment.

- Organizations rely heavily on tips for the initial detection of fraudulent activity, in part because of the high level of false positives from current analytic approaches.

- No matter how user-friendly tools and methodologies may be, skilled humans are still critical in the process, and these skill sets are expensive and often hard to come by for the federal government.
- New tools, approaches, and commercial data sets frequently appear that could help agencies combat fraud and other improper payments, but funding challenges often constrain agencies' ability to take advantage of them.
- Both pre-pay (before the payment is issued) and post-pay (after the payment is issued) analytics have value, but the greater value is with pre-pay analytics. The challenge to making investments in pre-pay analytics is the ability to measure their impact and use the outcomes to develop appropriate return on investment (ROI) metrics.
- Ongoing communication and information sharing among agencies can be critical to combatting common threats, but frameworks for doing this are not usually found across government.
- Capability maturity models can help agencies better understand the strengths and weaknesses of their use of data analytics in addressing Payment Integrity risks. However, there does not appear to be an accepted, standard data analytics capability maturity model in use across government.

DATA ANALYTICS CHALLENGES

Given the importance of analytics and the federal government's needs, one of MITRE's most important recommendations (#10 below) is for a shared, government-wide Payment Integrity research and data analytics capability.

Agencies and accountability organizations uniformly expressed the need for greater analytics capability, including people with key expertise and skills, as well as access to tools and various government, commercial, and open source data sets.

Recommendations: Preventing and detecting improper payments

We make the following recommendations.

6. Assess specific risks presented by the use of false (stolen, synthetic) identities.
7. Incorporate selected aspects of private sector KYC programs in agencies' identity validation processes.
8. Reduce reliance on self-reporting by benefit recipients where it causes the most risks.
9. Identify and pilot test agency-specific and government-wide alternatives for making identity and eligibility determination processes more rigorous, data driven, and cost-effective.
10. Establish a shared, government-wide research and data analytics capability – a Payment Integrity Research and Analysis Capability (PIRAC) – to enhance prevention and detection of improper payments (Figure ES-2). An important feature of the PIRAC would be evaluating alternatives for predictive and prescriptive modeling of future trends and their potential impacts on Payment Integrity to serve as an "early warning system" to help inform planning and prevention activities.

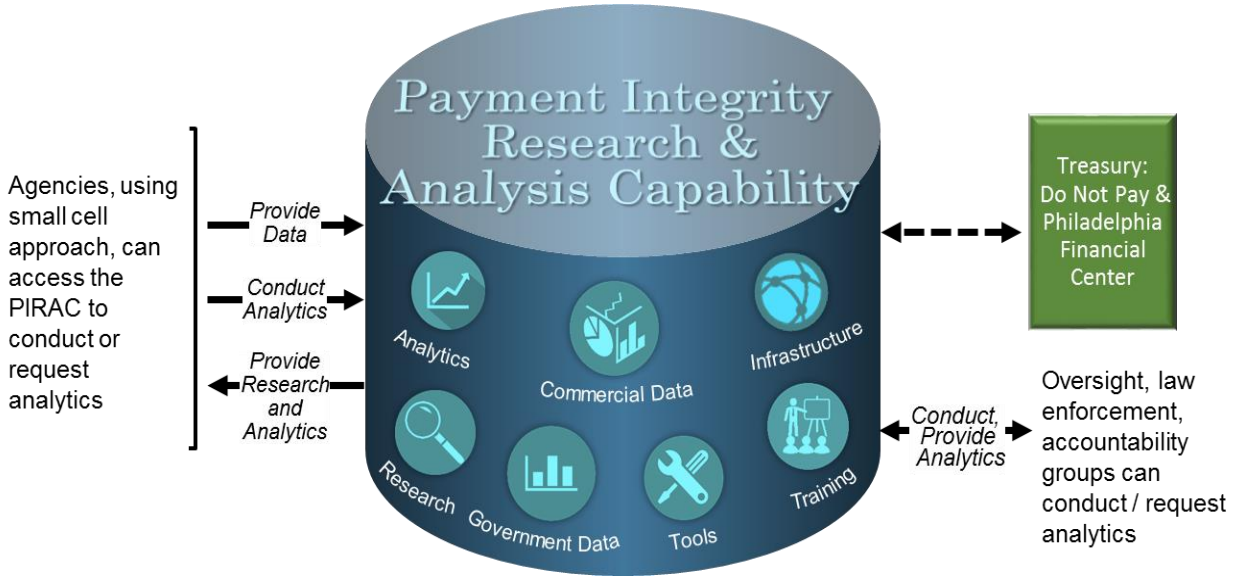


Figure ES-2. Payment Integrity Research and Analysis Capability

11. Establish an analytics capability maturity model for agencies to use in assessing their analytic capabilities and for identifying needed improvements.
12. Assess existing metrics to determine whether there are better ways to measure the ROI for pre-pay analytics.

If certain legislative, cultural, and technological obstacles cannot be overcome, then dramatic reductions in some improper payments may not be possible

Statutory provisions can create or exacerbate the potential for improper payments or reduce agencies' ability to resolve Payment Integrity problems by:

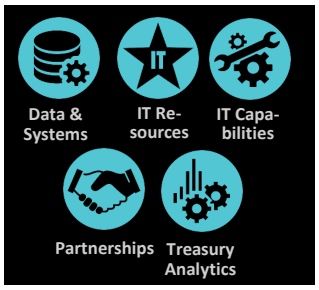
- Mandating aspects of the design of programs that create complications for Payment Integrity, such as by introducing risky or complex eligibility criteria
- Defining the same terms in different ways, thereby creating confusion for applicants and challenges for agencies in administering the programs; "household," for example, is defined differently for housing programs, for the Supplemental Nutrition Assistance Program, and for federal tax purposes
- Significantly restricting large-scale computer matching of data within and between agencies, including for the purpose of ensuring Payment Integrity

Some aspects of agencies' culture hinder the resolution of Payment Integrity challenges.

- As previously mentioned, agencies often experience a dilemma in key programs between making benefits payments at a certain time and making sure the payments are proper. Invariably they choose the former over the latter – a "mission over management" approach.

- Most agencies do not seem to have strong incentives to resolve Payment Integrity challenges internally or to assist other agencies with their challenges.
- Even when there are very common issues across programs, agencies usually believe their Payment Integrity challenges are unique. An emphasis on uniqueness perpetuates a "silo" mentality that can inhibit the identification of common issues and, potentially, systemic solutions.
- Most Offices of Inspector General take a "check the box" approach to their IPERA-mandated annual compliance audits, which is not as valuable as more comprehensively assessing their agency's reported root causes and corrective actions.

Finally, technology offers a critical line of defense in the fight against improper payments. On the other hand, technology can also be an enabler of financial crimes, in particular fraud; for example, the volume of income tax filing fraud has increased in recent years as electronic filing of individual tax returns has grown. The federal government faces a number of technology challenges in its fight against improper payments.



- Agencies are running a diverse set of legacy commercial and "home-grown" financial systems that use different computing environments and are not interoperable with each other.
- A frequent obstacle for the federal government, as well as the states, is the sufficiency of resources for information technology (IT).
- Some IT departments might feel challenged by their agency's needs for technology to help ensure Payment Integrity, such as analytics tools that might not be in their "sweet spot." The risk of failure could induce caution in procuring and enabling the use of anti-fraud commercial tools and data sets.
- Ecosystems surrounding government services – or for that matter, domains such as healthcare – are increasingly interconnected and involve multiple stakeholders and competing interests. The ability of any one organization or agency to accomplish meaningful change in these complex systems is limited by time, talent, and technology, among other factors.
- While implementation of the Digital Accountability and Transparency Act (P.L. 113-101) has driven some progress in the area of developing government-wide data standards, an even more comprehensive strategy could help reduce improper payments.
- The focus of the Treasury Department's Do Not Pay solution to date has been on stopping improper payments shortly before they are issued, and the future vision includes helping agencies identify potential improper payments earlier in processing. However, results through FY 2014 have been mixed with agencies reporting extremely high false positive rates, which Do Not Pay officials believe they have now addressed.

Recommendations: Legislative, cultural, and technological obstacles

We make the following recommendations.

13. Address statutes that appear to create or contribute to – via program design, definitions, etc. – improper payments in selected major programs.

14. Facilitate greater audit community impact on helping agencies reduce their improper payments.
15. Explore Public-Private Partnerships to cost-effectively bring to bear IT resources, data sets, and skill sets otherwise unavailable.

Figure ES-3 presents an overview of the current state in the three major issue areas of the study – federal government approaches to Payment Integrity; prevention and detection of challenging improper payments; and overcoming of legislative, cultural, and technology obstacles. Each of these is followed by its related recommendations, and then the desired future state that the recommendations are intended to help produce. In terms of priorities / next steps, the most critical actions to begin in the near future are establishing the government-wide leadership group, developing the risk management framework based on threat analysis, moving towards rigorous and data driven identity and eligibility determination processes, and establishing a government-wide Payment Integrity research and data analytics capability.

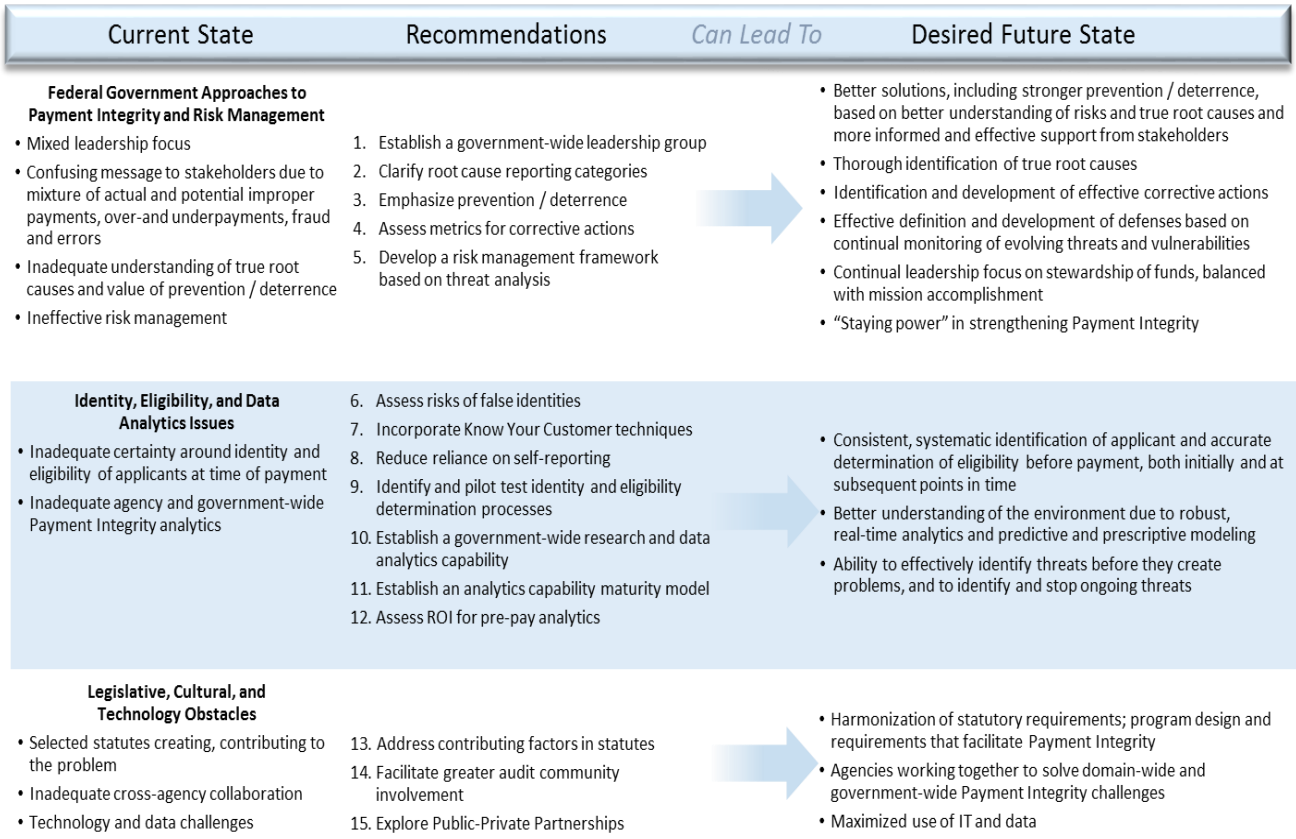


Figure ES-3. Envisioned Future State Will Better Ensure Government Payment Integrity

Table of Contents

1 Introduction 1-1
1.1 Improper Payments: A Longstanding Problem 1-1
1.2 Significance of Improper Payments 1-2
1.3 Uncertainty about the True Level 1-3
1.4 Payment Integrity Landscape 1-4
1.5 Recent Congressional and Executive Branch Focus 1-6
1.6 Key Questions Going Forward 1-8
2 Potential Future Trends and Their Implications for Payment Integrity 2-1
2.1 Environmental Trends 2-1
2.1.1 Economic Pressures 2-1
2.1.2 Healthcare Issues and Related Demographic Changes 2-3
2.1.3 Extreme Events 2-4
2.2 Technology Trends 2-5
2.2.1 Benefits, and New Risks, from Technology 2-5
2.2.2 Cyber-based Crime 2-7
2.3 Key Trends Driven by External Parties 2-9
2.3.1 Legislation 2-9
2.3.2 Behavior of Fraudsters 2-9
2.4 A Significant Problem Could Become Worse 2-10
3 How the Federal Government Approaches Payment Integrity Contributes to Sub-optimal Corrective Actions 3-1
3.1 Understanding the Improper Payments "Story" 3-3
3.2 Top Leadership Championing of Payment Integrity 3-3
3.3 Agencies' Approaches to Root Causes and Corrective Actions 3-5
3.4 "Applicant" vs. "Government" Actions Paradigm 3-7
3.5 Improper Payments Reporting Categories 3-9
3.6 What Agencies Can, and Cannot, Control 3-10
3.7 "Tension" Between Payment Integrity and Making Payments Promptly 3-11
3.8 "Commonalities" and "Convergence" Make Payment Integrity More Challenging and Complex 3-11
3.9 Conclusions 3-12
3.10 Recommendations 3-12
4 Effective Risk Management is Critical, Particularly Relating to Fraud 4-1
4.1 Current Approach Not Fully Facilitating Payment Integrity 4-1

4.2 Conclusions 4-2
4.3 Recommendation 4-3
5 Identity and Eligibility Risks Cut Across Many Agencies 5-1
5.1 Identity Concerns: Growing and Likely to Continue 5-1
5.2 Agencies Need Data to Verify Eligibility 5-2
5.3 Ongoing Research 5-4
5.4 Conclusions 5-4
5.5 Recommendations 5-4
6 Analytics Hold Great Promise, but Important Challenges Must Be Overcome 6-1
6.1 Significant Ongoing Analytics Activities 6-1
6.2 Analytic Approaches and Tools are Critical 6-2
6.2.1 Private Sector 6-2
6.2.2 Federal Government 6-3
6.3 A Number of Issues Challenge the Federal Government with Analytics 6-5
6.3.1 Organizations Rely Significantly on Tips vs. Analytics 6-5
6.3.2 Human Capital Issues 6-5
6.3.3 Analytic Environment Changing Rapidly, but Agencies Not Always Funded to Keep Up 6-5
6.3.4 Pre-pay Analytics: More Cost-effective than Post-pay but Harder to Cost-justify 6-6
6.3.5 Regardless of Tools and Methodologies, Data Can be a Problem 6-6
6.4 Communication and Information Sharing are Important 6-7
6.4.1 Maturity Models Generally Not Applied 6-8
6.5 Ongoing Research 6-8
6.6 Conclusions 6-9
6.7 Recommendations 6-9
7 Some Legislation Presents Barriers and Obstacles to Payment Integrity 7-1
7.1 Program Design 7-1
7.2 Definitional Issues 7-2
7.3 Prohibitions 7-2
7.4 Conclusions 7-3
7.5 Recommendation 7-3
8 Cultural Barriers and Obstacles Hinder Payment Integrity 8-1
8.1 Conclusions 8-2
8.2 Recommendation 8-2
9 Technology Barriers and Obstacles Need to Be Resolved 9-1

9.1 Data Standards and Systems Interoperability 9-1
9.2 IT Resources 9-2
9.3 IT Capabilities 9-2
9.4 Public-Private Partnerships 9-3
9.5 Do Not Pay and DATA Act Implementation 9-3
9.6 Conclusions 9-4
9.7 Recommendation 9-4
Appendix A Study Purpose and Methodology A-1
Appendix B Case Study – Medicare and Medicaid B-1
Appendix C Case Study – EITC C-1
Appendix D Case Study – Old-Age, Survivors, and Disability Insurance and SSI D-1
Appendix E Case Study – UI E-1
Appendix F List of Abbreviations F-1

List of Figures

Figure 1-1. Payment Integrity Landscape 1-5
Figure 1-2. The Fraud Triangle 1-6
Figure 3-1. Organizational Learning System and Interchange Media 3-2
Figure 3-2. GAO's Fraud Risk Framework 3-4
Figure 3-3. "Left of Check" vs. "Pay & Chase" 3-7
Figure 3-4. Segments of the Payment Integrity Assurance Process that the Federal Government Can Control, Guide / Oversee, or Influence 3-10
Figure 6-1. Shared, Government-wide Research and Data Analytics Capability: Conceptual Model 6-11
Figure 6-2. Shared, Government-wide Research and Data Analytics Capability: Conceptual High-Level Operation 6-12
Figure 6-3. Shared, Government-wide Research and Data Analytics Capability: Conceptual Detailed Operation 6-12

List of Tables

Table 1-1. Increases in Reported Improper Payments Dollars from FY 2007 to FY 2010 ($ in Billions) 1-2
Table 1-2. Major Congressional and Executive Branch Actions Addressing Improper Payments 1-6
Table 3-1. Root Causes and Corrective Actions by Issue Category 3-6
Table 3-2. Examples of Outreach and Prevention Efforts 3-8
Table 6-1. Selected Agency Best Practices as Presented in FY 2013 and 2014 AFRs 6-4

Table A-1. Study Interviews A-1
Table A-2. Study Guiding Principles A-7

1 Introduction

According to the Office of Management and Budget (OMB), the federal government annually makes more than $3 trillion in payments of all kinds – direct entitlement payments, grants, loans, acquisitions, and more. The great majority of payments are proper, i.e., made to the correct person or organization, at the right time, in the correct amount.

However, in fiscal year (FY) 2014 federal agencies, using their own methods and available data, estimated that there were nearly $125 billion in improper payments (4.0 percent of all payments) for 124 among the hundreds of programs. Considering the complexity of such estimates, the difficulty of estimating fraud, and the limited number of programs for which estimates are calculated, this may very well be a lower bound to the actual improper payments that year. Either way, this level of improper payments is unaffordable and adds to the current difficult economic picture.

Improper payments contribute to public concerns about the effectiveness of the government's stewardship over taxpayer dollars, making it more difficult for government to earn back the public's trust and potentially contributing to an increase in citizens' willingness to consider "cheating" on their taxes, benefits applications, etc. Recognizing that the level of improper payments will never be zero, it is reasonable to ask: What is a realistic, cost-effective level to which improper payments can be reduced? What level of "residual risk" – which could vary by program, agency, or domain – is reasonable to accept?

IMPROPER PAYMENTS DEFINED

The Improper Payments Elimination and Recovery Act of 2010 defines an improper payment as any payment that should not have been made or that was made in an incorrect amount (i.e., overpayments or underpayments).

1.1 Improper Payments: A Longstanding Problem

The overall amount of improper payments more than doubled over the last decade. Like the overall increase, in some cases the reported improper payments for individual programs jumped substantially.

- Medicare Fee-for-Service (FFS) – from $12 billion in FY 2005 to $46 billion in FY 2014
- Earned Income Tax Credit (EITC) – from $11 billion to $18 billion
- Medicaid – not estimated in FY 2005 to $18 billion
- Medicare Part C – not estimated in FY 2005 to $12 billion
- Unemployment Insurance (UI) – from $3 billion to $6 billion
- School Lunch Program and Medicare Part D – not estimated in FY 2005 to $2 billion

- Supplemental Nutrition Assistance Program (SNAP) – from $1 billion to $2 billion

The preponderance of the increase in the estimated dollars over the last decade took place from FY 2005 to FY 2010; amounts declined from FY 2010 to FY 2013 but then rose again from FY 2013 to FY 2014. Similar to dollars, the greatest rise in the reported improper payments rate occurred from FY 2007 to FY 2009; the rate declined from FY 2009 to FY 2013 but then rose again from FY 2013 to FY 2014. Table 1-1 highlights some of the more significant increases during just the FY 2007 – 2010 timeframe.

Table 1-1. Increases in Reported Improper Payments Dollars from FY 2007 to FY 2010 ($ in Billions)

Program	FY 2007	FY 2008	FY 2009	FY 2010
Medicare FFS	$11	$10	$31	$30
EITC	$11	$12	$12	$17
Medicaid	N/R	$19	$18	$23
Medicare Part C	N/R	$7	$12	$14
UI	$3	$4	$12	$17

Source: paymentaccuracy.gov

One reason for the overall increase is that improper payments are being estimated for more programs now than in FY 2005. For example, the number of programs being reported on jumped from 84 in FY 2013 to 124 in FY 2014 alone; the majority of this increase was due to the legislative requirement for agencies to estimate improper payments for federal payments related to Hurricane Sandy. Increasing federal dollars appropriated for many of these programs also contributed to the rise in the amount of the improper payments. Improved estimation methods might also account for some of the increase. Further, agencies that had been netting out recoveries of improper payments against the reported total were prohibited from doing so beginning in FY 2014.

1.2 Significance of Improper Payments

Regardless of the reasons for the increase, improper payments are a significant problem across government. They mean that a portion of the nation's limited funds is not available for the important purposes for which Congress appropriated them. In context, FY 2014's estimated improper payments of nearly $125 billion:

- Is the equivalent of the sixth largest federal agency – falling between the net cost of the Department of Agriculture (USDA) ($141 billion) and the Department of the Treasury ($103 billion)
- Represent almost 26 percent of FY 2014's $483 billion budget deficit
- Represent 29 percent of FY 2014's $431 billion interest on the national debt

Congress, OMB, agencies, cross-government councils like the Chief Financial Officers Council, and various other stakeholders are rightly concerned with the FY 2013 – 2014 jump in both the reported improper payments dollars (from approximately $106 billion to nearly $125 billion) and rate (from 3.5 percent to 4.0 percent). Questions exist regarding whether the reported dollars and rate may increase further. While everyone agrees that the dollars and rate are of concern, stakeholders sometimes differ in their points of view on what is causing these improper payments and what the possible solutions might be.

Leadership of The MITRE Corporation (MITRE), a not-for-profit organization that operates federally funded research and development centers (FFRDC) on behalf of federal government sponsors, recognizes the impact that the overall federal Payment Integrity situation has on government effectiveness and public confidence. Given the public interest nature of this challenge, MITRE conducted this independent, internally funded study to assess the underlying systemic factors that enable fraud and other improper payments and to explore government-wide solutions to improve Payment Integrity. In conducting this qualitative study, we researched over 120 public documents and interviewed officials at 13 agencies; 9 oversight and accountability organizations; 11 commercial, professional, and non-profit organizations; 2 universities; and a foreign government. See Appendix A for a complete description of the study methodology.

PAYMENT INTEGRITY DEFINED

Payment Integrity refers to improper payments and the people, processes, and technology that are meant to ensure that the payments are actually proper.

1.3 Uncertainty about the True Level

Despite extensive efforts in recent years to estimate and report on improper payments in individual federal programs, important questions remain about the nature of the improper payments themselves, most especially: what are the ***real*** numbers – the dollars, and the rate?

The Government Accountability Office (GAO) has reported concerns with the reliability of the improper payment estimates, indicating that the risk assessment and estimating methodologies are inconsistent among agencies. Beyond the 124 programs for which agencies estimated improper payments in FY 2014, numbers are not reported for the hundreds of other federal programs, including some significant ones like Temporary Assistance for Needy Families (TANF). In addition, the level of fraud is often unknown but can be significant. For example, while some experts maintain that nobody really knows how much fraud exists, private sector estimates for healthcare fraud alone range from 3 to 10 percent of expenditures, and the Association of Certified Fraud Examiners' 2014 global survey found that private sector organizations estimated an annual loss to fraud averaging 5 percent of revenues.[4] Further, private sector organizations often view fraud as a cost of doing business, so if costs go up, prices just go up. The government corollary, however, is that if the funds go missing, either taxes go up or there are fewer resources available for those for whom they were intended. Either way, while some level of fraud is no doubt included in the improper payments estimates, adding the unidentified fraud to the reported improper payments rate could cause it to increase significantly.

Overall, in its report on the FY 2013 – 2014 financial statements audit,[5] GAO cited the federal government's inability to determine the full extent to which improper payments occur, and to reasonably assure that appropriate actions are taken to reduce them, as a material weakness in the federal government's internal control.

[4] Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study (Association of Certified Fraud Examiners, 2014)

[5] U.S. Government's Fiscal Years 2014 and 2013 Consolidated Financial Statements (GAO-15-341R, February 26, 2015)

1.4 Payment Integrity Landscape

The Payment Integrity landscape is complex and expansive, creating many difficulties that lead to errors and opportunities that lead to fraud. As shown in Figure 1-1, various types of individuals and organizations apply for and receive a wide array of federal payments and benefits, from entitlement programs to tax refunds. When those applicants[6] commit fraud, there are almost always "commonalities" – accompanying "upstream" crimes (such as identity theft) and "downstream" crimes (such as tax evasion and money laundering).

Key elements of the landscape include the following processes and actors.

- Agencies often communicate with applicants before submission, and assist them during processing.
- Applications (e.g., claims for benefits, tax returns) are submitted to and adjudicated by agencies.
  - Applications can be proper / correct, erroneous, or fraudulent.
  - Processing can be proper / correct or erroneous.
- Many payments are compared to the data in the Treasury Department's Do Not Pay (DNP) solution shortly before being made to the applicants. Payments are either proper or improper.
- Applications suggesting indications of fraud are often investigated by law enforcement officials, and in some cases are prosecuted.
- In addition to agency staff working on a specific program, internal partners such as the financial (Chief Financial Officer [CFO]) and information technology (Chief Information Officer [CIO]) functions provide key assistance.
- External organizations provide mandates and guidance (e.g., Congress and OMB), and help ensure accountability (e.g., GAO and Offices of Inspector General [OIG]).
- External partner and value chain suppliers often provide key support, including FFRDCs and commercial vendors.

[6] In keeping with the IPERA definition of "payments," applicants refers to non-federal entities asking for / receiving a federal payment or service.

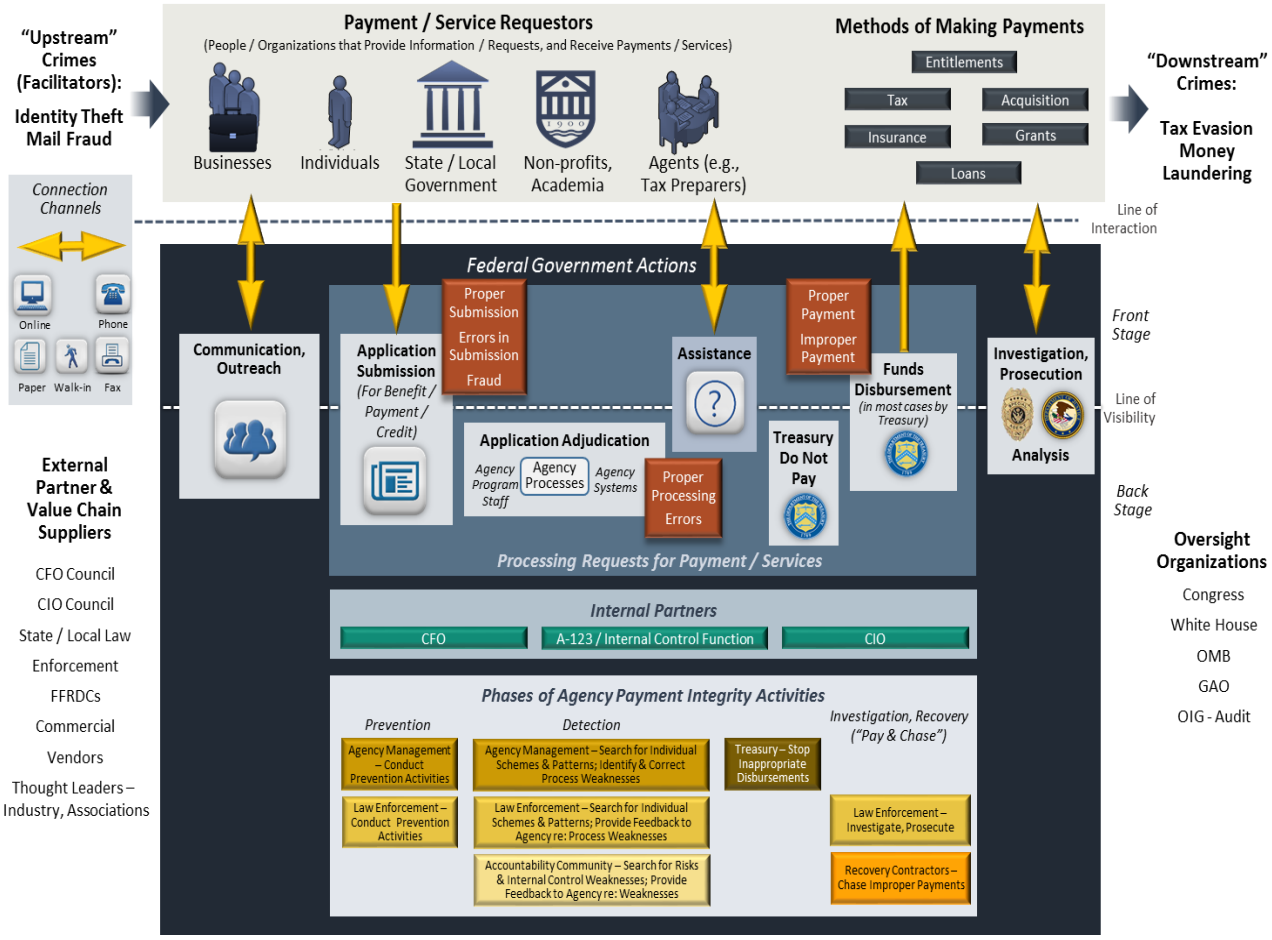


Figure 1-1. Payment Integrity Landscape

There are a variety of drivers to improper payments. First, actions committed by the parties involved – applicants (individuals, businesses, non-profit organizations, et al) and agencies – may drive such payments.

- Applicants may make errors – requesting a payment when they are not eligible for it or providing incorrect data with the request – without the willful intent to defraud. These often result from inadequate understanding of federal guidelines (e.g., must I report that income on my application? Can my business claim that cost on this contract invoice?). Applicants' understanding can, in turn, depend on the adequacy of agencies' communications.

- Applicants may commit fraud – attempting to intentionally defraud agencies in requesting payments or services. Fraud is deliberate and has a specific set of drivers, captured in the fraud triangle (Figure 1-2).

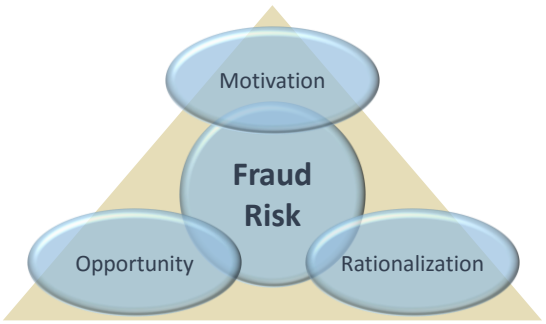


Figure 1-2. The Fraud Triangle

- Agencies may make errors – incorrectly determining applicants' eligibility or inaccurately calculating payment amounts – which often result from ineffective systems and processes. Their effectiveness depends on things like clear requirements (e.g., statutory language, OMB guidance, internal agency procedures); appropriate design (including strong internal controls), development, and implementation; availability of accurate information (e.g., to validate eligibility information provided by requestors); and staff training and skills.

Environmental drivers can dramatically impact the landscapes of an individual agency or program, as well as those of cross-government domains (e.g., healthcare, disaster response and recovery) and types of activities (e.g., procurement, grants). For example, healthcare Payment Integrity can be impacted by the following drivers.

- The political environment – The Patient Protection and Affordable Care Act (ACA) (P.L. 111-148) envisions paying for its mandates, in part, by reducing healthcare fraud and other improper payments. Tax credits available to help defray the costs to individuals are processed by both the Department of Health and Human Services (HHS) (the advance premium tax credit) and the Internal Revenue Service (IRS) (the premium tax credit).
- Complexity of the environment – Medicare has four major parts to be administered, with various contractors processing claims, operating systems, conducting program integrity investigations, and performing recovery audits. Medicaid is significantly funded by the federal government but administered by the states, which can introduce federal – state interface and relationship challenges.
- Types of entities being paid – These vary widely, from individuals to small businesses to major corporations, each with different legal requirements.

1.5 Recent Congressional and Executive Branch Focus

In recent years, the federal government has been giving increased attention to the challenges of Payment Integrity. Table 1-2 provides an overview of both Congressional and Executive Branch actions since 2002.

Table 1-2. Major Congressional and Executive Branch Actions Addressing Improper Payments

	Action	Payment Integrity-related Provisions
Congressional	Improper Payments Information Act of 2002 (P.L. 107-300)	Requires federal agencies to annually review all programs and activities and identify those that may be susceptible to significant improper

	Action	Payment Integrity-related Provisions
		payments, and for those programs and activities, estimate the annual amount of improper payments
	Fraud Enforcement and Recovery Act of 2009 (P.L. 111-21)	Clarified the definition of certain types of fraud and the intent of the False Claims Act (31 U.S.C. §§ 3729 - 3733), and authorized additional appropriations for the Department of Justice, the Department of Housing and Urban Development (HUD) OIG, and other organizations to combat these types of fraud
	Improper Payments Elimination and Recovery Act (IPERA) of 2010 (P.L. 111-204)	Requires federal agencies to periodically review and report on major programs that are susceptible to improper payments
	Improper Payments Elimination and Recovery Improvement Act (IPERIA) of 2012 (P.L. 112-248)	Establishes the DNP Initiative and requires federal agencies to ensure that a thorough review of available databases with relevant information on eligibility occurs to determine program or award eligibility and prevent improper payments
	Digital Accountability and Transparency Act (DATA Act) of 2014 (P.L. 113-101)	Authorizes the Secretary of the Treasury to establish a data analysis center, or expand an existing service, to provide data, analytic tools, and data management techniques to support, among other things, the prevention and reduction of improper payments; and transfers the assets of the Recovery Accountability and Transparency Board's (RATB) Recovery Operations Center (ROC) to Treasury upon the establishment of the data analysis center
Executive Branch	Executive Order 13520, *Reducing Improper Payments and Eliminating Waste in Federal Programs* (November 20, 2009)	Establishes a strategic outcome, goals and strategies for reducing improper payments
	OMB Memorandum M-10-13, *Issuance of Part III to OMB Circular A-123, Appendix C* (March 22, 2010)	Provides guidance for estimating improper payments and for recovery auditing
	Presidential Memorandum, *Enhancing Payment Accuracy Through a "Do Not Pay List"* (June 18, 2010)	Directs agencies to review prepayment and pre-award procedures and ensure that a thorough review of available databases with relevant information on eligibility occurs before the release of any federal funds, including five specific databases collectively called the "Do Not Pay List"
	OMB Memorandum M-12-11, *Reducing Improper Payments through the "Do Not Pay List"* (April 12, 2012)	Discusses the Treasury DNP solution, the RATB's "Fast Alert," and the Government Accountability and Transparency Board's call for "a centralized fraud framework to track and oversee federal spending"

	Action	Payment Integrity-related Provisions
	OMB Memorandum M-13-20, *Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative* (August 16, 2013)	Provides guidance to implement IPERIA and to help federal agencies protect privacy while reducing improper payments with the DNP Initiative

Source: MITRE Analysis of Identified Documents

1.6 Key Questions Going Forward

We acknowledge the considerable efforts already in place at OMB and across federal agencies focused on identifying, reporting and mitigating improper payments. This study seeks to provide useful input and new insights to those efforts by addressing these key questions:

- What trends may be coming that could adversely impact the rate or the total dollars of improper payments?
- What are the root causes of the current improper payments?
- What obstacles must be addressed to make greater progress towards solutions?
- How can the federal government attack the problem in more effective, proactive ways?

The time has come for broader, cross-government approaches and transformational solutions, and with that in mind, the following sections address these key questions.

2 Potential Future Trends and Their Implications for Payment Integrity

A number of known and anticipated trends will likely have future implications for improper payments – from increasing the magnitude of payouts by programs that have difficulty preventing improper payments (thereby increasing the overall dollars of improper payments made, even if the rate remains constant), to creating or increasing vulnerabilities to applicant or agency processing errors, to creating or increasing threats from fraud. This study addresses trends in the following areas.

- Economic pressures
- Healthcare issues and related demographic changes
- Extreme events
- Technology risks
- Cyber-based crime
- Legislation
- Behavior of fraudsters

2.1 Environmental Trends

2.1.1 Economic Pressures

Economic pressures from the overall growth in the national debt and federal budget deficits, along with declining labor force participation, have expanded the number of people participating in means-tested benefits programs and potentially provide incentives for fraud. Just as with healthcare, the magnitude of dollars involved with programs like UI and Supplemental Security Income (SSI) means that even if the rate of improper payments remains constant, as payments climb the dollar value of improper payments could increase significantly. Specific trends of concern include the following.

- Slowed economic growth – The Congressional Budget Office (CBO) has projected that the 2018 – 2024 Gross Domestic Product (GDP) growth will be notably less than the average growth during the 1980's and 1990's.[7]

[7] An Update to the Budget and Economic Outlook: 2014 to 2024 (Pub. No. 5005, August 27, 2014)

- Climbing federal expenses and national debt
  - CBO projects debt and deficits to climb.[8]
  - By 2039, CBO projects federal spending will increase to 26 percent of GDP, while debt held by the public will likely exceed 100 percent of GDP.[9]
  - GAO has indicated that net interest payments are expected to grow significantly.[10] Absent revenue increases, this will reduce funding available for other federal programs and make "competition" for the available dollars stiffer.
  - CBO expects annual federal outlays to increase 5.2 percent each year, due in part to the mounting interest on federal debt.[11]
  - Ongoing economic challenges bring increased priority and urgency to government efforts directed at closing the tax gap, while potentially motivating more people to commit fraud in order to receive funds from a shrinking pool of available government resources.

INCREASING SPENDING AND DEBT

According to the CBO, federal spending, debt and deficits are expected to continue to climb, while the labor force participation rate continues to fall.

- Declining labor force participation rate – While the reported unemployment rate has been falling, CBO projects the labor force participation rate to continue to decline.[12]
- Declining mean and median net worth and mean household incomes
  - The Census Bureau (Census) reported that the percentage (as well as the number) of people in poverty and living in poverty areas increased from over 18 percent in 2000 to almost 26 percent in 2010, accompanied by problems such as higher crime, fewer job opportunities, and poor housing.[13] If this trend continues, it could place greater pressure on means-tested benefit programs.
  - Census also reported a decline in the share of households represented by married couples with children under 18 from 40 percent in 1970 to 20 percent in 2012. "Other family" households (house-holder living with children or other relatives but no spouse present) increased from 11 percent to 18 percent during this period. Married families tend to be economically advantaged compared with other families.[14] If this trend continues, it could, again, further stress means-tested benefit programs.
  - The Congressional Research Service (CRS) has reported the poverty rate for illegal immigrants is notably higher than the national average.[15] A legal path to citizenship may increase the number of people getting entitlement payments.

[8] An Update to the Budget and Economic Outlook: 2014 to 2024 (Pub. No. 5005, August 27, 2014)
[9] The 2014 Long-Term Budget Outlook (Pub. No. 4933, July 15, 2014)
[10] Anticipating and Meeting Accountability Challenges in 2014 and Beyond (GAO-14-591CG, May 20, 2014)
[11] An Update to the Budget and Economic Outlook: 2014 to 2024 (Pub. No. 5005, August 27, 2014)
[12] An Update to the Budget and Economic Outlook: 2014 to 2024 (Pub. No. 5005, August 27, 2014)
[13] Changes in Areas With Concentrated Poverty: 2000 to 2010 (ACS-27, June 30, 2014)
[14] America's Families and Living Arrangements: 2012 (P20-570, August 2013)
[15] Noncitizen Eligibility for Federal Public Assistance: Policy Overview and Trends (RL33809, September 27, 2012)

Both CBO[16] and CRS[17] have raised the possibility that absent corrective actions in the near term, a severe fiscal crisis is inevitable, which would only exacerbate the existing challenges.

2.1.2 Healthcare Issues and Related Demographic Changes

Healthcare issues and related population demographic changes are increasing the demand on and straining existing healthcare and age-related means-tested benefits programs. The magnitude of dollars involved with programs like Medicare and Medicaid means that even if the rate of improper payments remains constant, as payments climb the dollar value of improper payments could increase significantly. Further, healthcare fraud has been increasing in recent years, and there are no indications that it is slowing.

Industry experts believe that up to 30 percent of the U.S. healthcare industry's spending is lost to fraud, waste or abuse.[18] With America's healthcare expenditures projected to exceed $4 trillion in 2016, the absolute dollar impact of fraud, waste and abuse could exceed $1 trillion. The greatest financial leakage does not appear to be from outright fraud, which is estimated to constitute 3 to 10 percent of total healthcare spending, but rather from waste and abuse, which may constitute 20 percent or more.

Specific trends of concern include the following.

- Aging population
  - Life expectancy may increase in the near future – possibly by 6 months – due to widespread adoption of wireless health monitoring technology.
  - Longer life spans will likely present greater healthcare needs and, over time, more long-term care.

[16] The 2014 Long-Term Budget Outlook (Pub. No. 4933, July 15, 2014)
[17] The Federal Budget: Overview and Issues for FY2015 and Beyond (R43472, April 11, 2014)
[18] Fraud, waste and abuse have been defined in various ways. In general, fraud is a type of illegal act involving the obtaining of something of value through willful misrepresentation. Waste involves taxpayers not receiving reasonable value for their money in connection with government funded activities due to an inappropriate act or omission by individuals with control over or access to government resources; most waste does not involve a violation of law but rather primarily relates to mismanagement, inappropriate actions and inadequate oversight. Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances; it includes misuse of authority or position for personal financial interests or those of an immediate or close family member or business associate but does not necessarily involve fraud, violation of laws, regulations, or provisions of a contract or grant agreement. (see http://www.dodig.mil/resources/fraud/fraud_defined.html)

- CBO has reported that the Disability Insurance and Old-Age, Survivors Insurance trust funds are expected to be exhausted in the near future, primarily due to demographics.[19]

- Dramatic increases in participation in, and spending for, healthcare programs – CBO has projected that annual federal outlays will increase 5.2 percent each year, due in part to aging, expanding federal subsidies for health insurance, and rising healthcare costs.[20]
- Electronic health records could open doors to more / new types of fraud.
- Underreporting of income in ACA marketplaces in order to qualify for subsidies is of concern.

KEY TRUST FUNDS AT RISK

CBO expects the Old-Age, Survivors Insurance trust fund to be exhausted by 2033. The Bipartisan Budget Act of 2015 extended the expected life of the Disability Insurance trust fund, but only to 2022.

The two largest federal healthcare programs, Medicare and Medicaid, are on GAO's High Risk list. GAO's February 2015 *HIGH-RISK SERIES An Update* makes the following points about the ability of the Medicare and Medicaid programs to combat improper payments.

- *The Medicare integrity program – along with other activities to detect, prevent, and combat factors that contribute to improper payments – is funded through the Healthcare Fraud and Abuse Control program. In [FY] 2015, Congress provided more than double the prior year's discretionary Medicare integrity funding… [However, the Centers for Medicare & Medicaid Services (CMS)] experienced less favorable funding in prior years, including a 6 percent decline in discretionary Medicare integrity funding from [FY] 2011 to 2014…indicat[ing] an uncertain budgetary environment.*
- *[For Medicaid,] CMS…needs to address emerging areas where fundamental gaps in oversight capacity exist. For example, many Medicaid beneficiaries receive services under managed care, and states' use of managed care is expected to increase significantly over the next 5 years, yet CMS and states lack effective program integrity systems for care delivered by managed care organizations. Similarly, in 2012, approximately 13 percent of Medicaid enrollees had private health insurance and the number of Medicaid enrollees who also have private health insurance is expected to increase with the expansion of Medicaid.* [21]

2.1.3 Extreme Events

Extreme events can demand increased provision of services and benefits, e.g., in responding to and recovering from damaging hurricanes. These can be very susceptible to fraud, waste and abuse. Specific trends of concern include the following.

- Natural events such as disasters and climate-related risks – GAO has reported that "During the 10 fiscal years from 2004 through 2013, Presidents declared 32 percent more major disasters than in the preceding 10 fiscal years."[22]

[19] The 2013 Long-Term Projections for Social Security: Additional Information (Pub. No. 4796, December 17, 2013)
[20] An Update to the Budget and Economic Outlook: 2014 to 2024 (Pub. No. 5005, August 27, 2014)
[21] HIGH-RISK SERIES An Update, GAO-15-290, February 11, 2015
[22] FEDERAL EMERGENCY MANAGEMENT AGENCY Opportunities Exist to Strengthen Oversight of Administrative Costs for Major Disasters (GAO-15-65, December 17, 2014)

- GAO has expressed concern about increasing instability and the potential for further proliferation of nuclear, biological, and chemical weapons.[23]
- Wars and other conflicts (such as those from terrorism) drive demand for funding, as do some of their impacts (e.g., human migrations from the ongoing Middle East conflicts).

Managing climate change risks, in particular, is on GAO's High Risk list. The February 2015 *HIGH-RISK SERIES An Update* makes the following points.

- *[G]overnment-wide improvement is needed to reduce fiscal exposure [in areas] including, but not limited to, the federal government's role as…the insurer of property and crops vulnerable to climate impacts; and the provider of aid in response to disasters.*
- *Multiple factors, including increased disaster declarations, climate change effects, and changing development patterns increase federal fiscal exposure to severe weather events…Such federal disaster aid functions as the insurance of last resort in certain circumstances because whatever is not covered by insurance or built to be resilient to extreme weather increases the federal government's implicit fiscal exposure through disaster relief programs.*
- *As long ago as 1980, we reported that individuals may not act to protect themselves from the effects of severe weather if they believe the federal government will eventually help pay for their losses.*[24]

2.2 Technology Trends

2.2.1 Benefits, and New Risks, from Technology

Technology can be of great help in addressing the government's Payment Integrity challenges, by means of data analytics tools and approaches, access to an expanding array of data, and more. The IRS, for example, has found the increased level of information reporting in recent years to be very helpful in ensuring tax compliance and expects that trend to continue. On the other hand, experts indicate that financial crime today is increasingly complex and technology-driven, and technology introduces new risks (e.g., increasing ways to access government systems). Specific trends of concern include the following.

- Spread of mobile internet and electronic payment and "value" systems
    - Experts believe that digital currencies, online communication tools, social and gaming networks, mobile devices like smart phones and tablets, and even space-based approaches to money storage are opening up more and more avenues for storing and transferring "value."
        - Some online role-playing games have begun incorporating the ability to convert real-world currency into "virtual value" that could be used to purchase items in the game. Money launderers are moving value to and from a virtual world, enabling funds to easily cross national borders and providing an effective means to place and layer[25] illicit proceeds.

[23] Anticipating and Meeting Accountability Challenges in 2014 and Beyond (GAO-14-591CG, May 20, 2014)
[24] HIGH-RISK SERIES An Update (GAO-15-290, February 11, 2015)
[25] Money laundering consists of three activities: placement (introducing illegal profits into the financial system), layering (engaging in a series of conversions or movements of the funds to distance them from their source), and integration (re-entering the funds into the legitimate economy).

        - Virtual worlds have almost no oversight from any regulatory body. A 2012 European Central Bank report on currency trading in virtual worlds stated: "Every criminal act which takes place in the real world might also be reproduced and adapted to…virtual communities. But the likelihood is even stronger as a result of the lack of proper regulation and oversight and owing to the high degree of anonymity that exists in these online worlds."[26]
        - Growing fears about cybersecurity have spawned satellite-based data centers that could contain digital money immune to physical hacking. For example, Bitcoin data servers are partnering with Deep Space Industries to acquire craft to ferry 24 small satellites into space. The orbital "safety deposit boxes" would be impervious to any law enforcement agency, regulator or tax collector, raising concerns about their potential use for money laundering.
    - A Lexis-Nexis study found that between 2013 and 2014, the number of private sector retailers offering customers a mobile commerce (m-commerce) option doubled from 7 to 15 percent, but m-commerce fraud is growing at an even faster rate.

- Advances in computer capabilities: Cognitive analytics, Artificial Intelligence, machine learning, natural user interfaces, etc.
    - With rekindled interest and investment in Artificial Intelligence, rapidly expanding computer power, and evolving theories such as "disruptive innovation,"[27] some experts believe that computer algorithms themselves will soon be conceiving significant, disruptive products. Further, competing autonomous algorithms that ran unchecked caused the 2011 stock market "flash crash." If algorithms are able to do those things, will they be able to conceive of new ways to commit fraud that could be more difficult than ever to detect?

TECHNOLOGY CAPABILITIES

Technology capabilities continue to increase and expand, bringing both solutions and new risks.

    - Experts believe that sophisticated organized crime and fraud rings might use cognitive systems to commit frauds in ways that appear normal to automated detection systems.
- Disruptive technologies – particularly the Internet of Things (IoT)
    - By 2020, some experts predict that there could be 70 billion "things" (refrigerators, cars, etc.) connected to the internet; the number is growing faster than other technology like Smartphones.
    - Security is a significant IoT risk – in fact, the biggest concern – for organizations. Threats arise from breaches, leaks, and exploits. Authentication and security of the "thing" itself, and validating user identity, are significant problems. "Things" can be easily located using internet search tools, e.g., Shodan, and then exploited.

[26] Virtual Currency Schemes (European Central Bank, October 2012)
[27] "Disruptive innovation" refers to an innovation transforming an existing industry by introducing simplicity, convenience, accessibility, and affordability that can replace complication and high cost. A disruptive innovation initially forms in a niche market but eventually the innovation can completely redefine the entire industry.

- Experts indicate that the availability of digital technology and Generation Z's obsession with the IoT are changing expectations and increasing the demand for agile access to data and resources. If, over time, government programs open access to a wider array of entry points to accommodate these changing expectations, then fraudsters will likely find new ways to access federal systems and perpetrate schemes.

- Electronic interfaces with government
  - Electronic interfaces with government have been growing and are likely to continue to increase. For example, in 2012, 80 percent of individual income tax returns were electronically filed, reaching the goal Congress set in 1998.
  - Simultaneously, industry is working to maximize the "serve yourself" ability of consumers by making processes more intelligent, as well as by minimizing manual interventions. A government move in this same direction would call for increased error and fraud detection built into processes as a result of decreased human oversight.

- Experts have indicated that some technologies instituted as program improvements or internal controls can actually be high risk in themselves, e.g., prepaid (re-loadable) cards that can be misused for fraud or money laundering.

- People skills
  - Prognosticators believe that some traditional human IT roles – developer, system engineer, software tester – will be at least partially replaced by "smart machines," incorporating machine learning and cognitive technologies to make processes faster and more efficient. Humans will need to be able to work with these smart machine technologies, but such skills are rarely available today and are not being widely taught in educational institutions.
  - Science, technology, engineering, and mathematics graduate shortages are well known, and enrollment in science programs has declined in recent years, indicating that these shortages will likely continue. Experts have stated that "people issues" – especially the types of skillsets on hand – are often bigger obstacles to fighting fraud than technology challenges.

2.2.2 Cyber-based Crime

Cyber-based crime is increasing due to low cost of entry and ease of execution, and government programs are especially vulnerable. In fact, it is much easier and cheaper for a cybercriminal to launch an attack than it is for an agency to defend against one. Today it is cheaper than ever for hackers to purchase ready-made attacks, rent botnets and even buy or create complex malware via a software subscription service, complete with 24 / 7 customer support. Specific trends of concern include the following.

- Identity theft
  - The increasing prevalence of stolen identities makes it much easier for individuals to claim benefits from government programs, as well as from private companies, because having a solid identity makes it harder to separate a true identity from a false one. The Office of Personnel Management (OPM) data breach, for example, may have released information on more than 21 million current and former federal employees – names, addresses, and other details of federal employees' entire families,

such as mothers' maiden names, that might be asked when changing supposedly "lost" passwords, as well as information from which the answers to many other questions that appear in such security systems can be deduced. This data could help in the creation of millions of apparently legitimate identities.

- IRS reported that it detected 642,000 cases of identity theft in the first 9 months of 2012, up from 242,000 in all of 2011. The figure does not include 436,000 fraudulent refund claims filed in 2012 using the Social Security numbers (SSN) of Puerto Rican citizens.
- Some experts believe that existing identifiers (names, SSNs) are not strong enough for reliable verification, and as yet, other solutions around approaches such as biometrics are fairly limited.

- Volume and types of attacks
  - A 2014 global study by PricewaterhouseCoopers showed that the number of detected cyberattacks skyrocketed in 2014 – up 48 percent from 2013.
  - Experts have stated that hackers are obtaining more and more information by attacking more and more systems, especially non-financial systems. For example, healthcare records are extremely valuable for non-healthcare fraud uses.
  - International cyber threats are significant and growing, with nation state attacks growing in volume and sophistication. Russian and Eastern European criminal organizations, in particular, are increasingly attacking U.S. systems, with their countries often profiting.
  - Experts indicate that the capabilities of threat actors are increasing, from simply using pre-existing vulnerabilities in widely used software or organizations' systems, to identifying and exploiting new vulnerabilities, and now to actually creating vulnerabilities.

IDENTITY THEFT AND TAX FRAUD

During the 2015 tax filing season, the Alabama Department of Revenue official in charge of income tax fraud prevention had his identity stolen and a refund return filed in his name. Technology advances complicated the situation, with the official indicating that automating and increasing the speed of the tax refund process make it far easier for criminals to commit fraud quickly.

One of GAO's High Risk categories is security of federal information systems and cyber-critical infrastructure and protecting the privacy of personally identifiable information (PII). GAO's February 2015 *HIGH-RISK SERIES An Update* makes the following points.

- *[C]yber threats and incidents to systems supporting the federal government and national critical infrastructures are increasing. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, advanced persistent threats – where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives – pose increasing risks. Further underscoring this risk are the increases in incidents that could…lead to inappropriate access to and disclosure, modification, or destruction of sensitive information.*

- *[T]he federal government continues to face challenges in effectively addressing increasing concerns about the protection of the privacy of…PII. The number of reported security incidents involving PII at federal agencies has increased in recent years, rising from 10,481 incidents in 2009 to 27,624 incidents in 2014.*
- *In addition, the recent high-profile breaches of PII at federal agencies and commercial entities have heightened concerns that personal privacy is not being adequately protected. For example:*
    - *In September 2014, a cyber intrusion into the United States Postal Service's information systems may have compromised PII for more than 800,000 of its employees.*
    - *Credit and debit card information of 56 million customers of Home Depot, Inc. may have been compromised in a 5-month attack on its payment terminals.*[28]

2.3 Key Trends Driven by External Parties

2.3.1 Legislation

Statutes are increasingly impacting the relationships between government programs. A trend of concern is the growing interrelationship / duplication / overlapping of programs.

- Despite the frequent interrelationship / duplication / overlapping of programs, agencies usually look at Payment Integrity in their individual agency or program stove-pipes.
- The ACA creates an unusual "pipeline" between two agencies – HHS and IRS – for payment of the premium tax credit designed to help make purchasing health insurance coverage through the Health Insurance Marketplace more affordable. For eligible individuals, HHS can provide an advance credit payment sent directly to their insurer; alternately, individuals can claim the premium tax credit when filing their tax returns. Unlike other federal programs where only one agency is responsible for identifying and addressing improper payments in the program, in this new structure two agencies must collaborate to do so.

2.3.2 Behavior of Fraudsters

Fraudsters' behavior is increasingly sophisticated, changing, and ubiquitous. Technical advancements and the globalization of fraud will continue to provide increasing challenges to organizations' ability to manage fraud in all of its manifestations. Specific trends of concern include the following.

- Greater professionalization of fraud practices through smarter attacks (especially online) results in bigger payoffs, which then attracts more talented thieves.
- Increasing hostility and boldness of organizations and individuals – Fraudsters are increasingly attacking government infrastructure and creating open challenges to public institutions (e.g., large scale tax fraud and identity theft).

[28] HIGH-RISK SERIES An Update (GAO-15-290, February 11, 2015)

- Sharing practices in their "community" – Fraud practices are increasingly being shared from fraudster to fraudster, often facilitated by online communications and the darknet.
- Increasing technical / cyber issues interwoven with, and enabling, fraud – Technical skills such as hacking are increasingly going hand-in-hand with more traditional fraud skills.
- Organized crime, drug cartels, and even low level drug traffickers are increasingly involved in fraud schemes.
- Growing internationalization
  - More frauds are being perpetrated from offshore locations.
  - More frauds are leading to offshore money laundering.
- Healthcare fraud – Experts estimate it to be between 3 and 10 percent of all medical expenditures; federal healthcare improper payments, which likely include some fraud, account for over 60 percent of the FY 2014 reported improper payments.
  - Small-dollar-per-instance fraud is growing and is likely to continue and even accelerate because of the disruption in the marketplace caused by the implementation and expansion of the health insurance exchanges.
  - This growing low-dollar fraud is challenging all payers to address the emerging threat from nonmedical professional fraudsters, and healthcare fraud is expected to continue moving outside of local provider networks.
- Increasing rationalization of fraud – According to recent academic research, societal acceptance of white collar crime in general has been growing. If this trend continues, then willingness to commit fraud could increase.

HEALTH INSURANCE EXCHANGES FRAUD

IDC Health Insights reports that "Perpetration of fraud by 'consumers'…increased rapidly [since 2005]. This is very likely to continue to increase as perpetrators take advantage of disruption caused by the implementation of consumer-oriented health insurance exchanges." (Business Strategy: U.S. Healthcare Payer Fraud, Waste, and Abuse Solutions Marketplace Overview, IDC Health Insights, May 2014)

2.4 A Significant Problem Could Become Worse

Each of these trends is already occurring to some degree, but their precise impact on future improper payments is difficult to project without an informed analysis of relevant data. Further, other, currently unanticipated, trends may surface. That said, there is the potential that the already significant government improper payments problem could worsen because of these trends, calling for proactive consideration of these potential events and thoughtful attention to what should be done to mitigate their impact.

3 How the Federal Government Approaches Payment Integrity Contributes to Sub-optimal Corrective Actions

Albert Einstein is often quoted as saying "If I had an hour to solve a problem I'd spend 55 minutes thinking about the problem and 5 minutes thinking about solutions." The corollary for improper payments is that it is critical to understand true root causes in order to formulate effective corrective actions. In other words, how well the government identifies the root causes of improper payments contributes to framing the right corrective actions to address them. Discussions with a wide range of people, from GAO to academicians, echoed this.

Understanding how organizations approach information is key to ensuring that the true root causes of improper payments are addressed with the right corrective actions. Much like individuals develop and use mental models to process information, organizations develop and use schemas to filter information. Schemas are based on the idea of a dominant logic that brings together previous experiences to help form the culture of the organization. Schemas provide links to the past by transforming and recognizing incoming information based on past experience and then plugging it into the organization. They provide a kind of general outline of a scene from experience, with many positions left blank and details to be filled in by ongoing experience. This creates an organizational mindset that may avoid or even ignore information that does not fit the current schema – where information that creates dissonance for the organization is set aside in favor of the status quo.

For organizations such as federal agencies or the government as a whole to approach Payment Integrity differently, it is helpful to understand how they take in new information and turn it into new schemas or mental models. In their book *Organizational Learning: From World-Class Theories to Global Best Practices*, David Schwandt and Michael Marquardt illustrate how four subsystems within organizations work (see Figure 3-1).[29]

[29] From Schwandt, D.R., Organization learning, in *Advances in Strategic Management*, Vol. 14, Walsh, J.P. and Huffs, A., Eds., JAI Press, Stamford, CT, 1997.

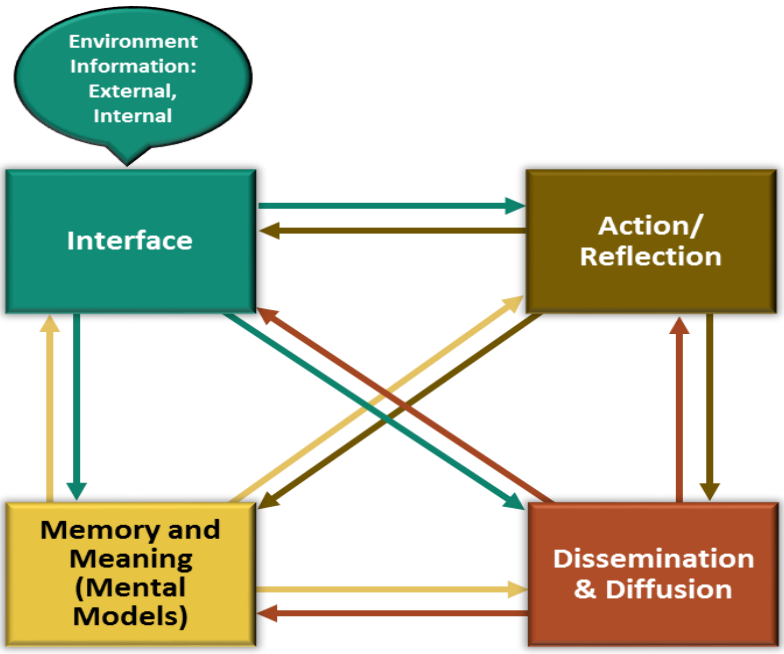


Figure 3-1. Organizational Learning System and Interchange Media

At a high level, the four subsystems work together in order for an organization to interact both externally with the environment around it, and internally within itself. The Interface subsystem's role is to receive information, in particular new information, from the environment. The Action / Reflection subsystem tests that information against the goals of the organization, while the Dissemination and Diffusion subsystem shares the validated information across the organization. Finally, the Memory and Meaning (Mental Models) subsystem's role is to change organizational behavior so that the new information becomes part of the way the organization operates.

However, changing the way an organization operates requires disconfirming evidence. An organization's memory and meaning (or schema) is designed to stabilize the organization and thus it requires the most energy to change. In fact, it is designed to dismiss most of the information in the external environment that does not fit the organization's schema. Understanding this structure of organizations is critical to Payment Integrity so that organizations:

- Seek and receive complete, accurate information about the true root causes of improper payments
- Understand those true root causes in the context of the goals of the overall organization or of a specific program
- Structure corrective actions to address those true root causes in order to change systems, processes, and the behavior of people to reduce improper payments

Changing the way an organization as large and complex as the government approaches an issue like Payment Integrity is no small task. It requires, among other things, presenting clear evidence to better tell the story of improper payments. This will help organizations shift their mental models in order to reduce improper payments.

3.1 Understanding the Improper Payments "Story"

The way the federal government currently categorizes and reports improper payments can confuse stakeholders. First, the reporting of improper payments includes both actual and potential improper payments, all of which stakeholders seem to "hear" as actual, judging by news accounts and political commentary. Further, the definition of improper payment includes underpayments as well as overpayments, so not all improper payments represent a loss to the government; yet stakeholders, again, seem to "hear" all improper payments as government waste and loss. Finally, it seems unclear to many stakeholders that improper payments consist of not just fraud, but also applicant errors and government processing errors; public discussion around improper payments frequently characterizes them all as fraud.

3.2 Top Leadership Championing of Payment Integrity

The message sent by top leadership of an organization is absolutely critical to ensuring Payment Integrity. Private sector best practices stress the importance of an organizational philosophy that fraud, waste and abuse is considered to be a problem, with key attributes such as the following supporting that philosophy.

- A Payment Integrity unit exists, is not buried in the organization structure, and is adequately resourced.
- The human component is recognized as an important part of the Payment Integrity program; i.e., the organization cannot rely exclusively on technology to identify and resolve improper payments.
- Certain skillsets should be present, including technical expertise, domain knowledge, and law enforcement.

Academic research has demonstrated that what is called "tone at the top" is critical to Payment Integrity. Leadership must talk about the unacceptability of fraud, waste and abuse, both within the organization and from outside. Communication about the topic must be regular – not a singular event like an annual email. Research has shown that the right "tone at the top" can increase employee attention to the potential for external fraud; this "tone" will not necessarily make employees better at identifying fraud, but it will at least make them less tolerant of it. Further, the right "tone at the top" can decrease insider threat from fraud, as well as reduce waste and abuse.

Agency officials commented that both within their agencies and government-wide, they are looking for top leadership to "own the problem" and send a strong message about resolving improper payments. One way to facilitate this would be to establish a Cross-agency Priority Goal. This would serve notice across the federal government that taking action – both at the individual agency level and across domains and the entire government – is critical and expected. Establishing such a goal would be an important step in carrying the issue forward into the next Administration.

In some agencies Payment Integrity is viewed as a CFO issue, while in others multiple executives are responsible for different aspects like reporting, operations and execution management. Top leadership emphasis across agency components is critical; for example, Social Security Administration (SSA) officials advised us that their top leadership has assumed a prominent role, both internally and externally, to further improve Payment Integrity. First, they

have worked internally to cut across organizational and program silos by promoting extensive cooperation to address Payment Integrity issues. The Office of Data Exchange and Policy Publication centralizes access to and sharing of data inside SSA. Leadership has established an Improper Payments Oversight Board to help clarify roles, promote understanding of accountability SSA-wide, reinforce shared responsibilities for solving improper payments problems, and shape Payment Integrity strategies and program portfolios to ensure a targeted approach and alignment with major sources of improper payments. SSA also initiated and leads a government-wide Federal Data Exchange Community of Practice, and they collaborate with HHS, USDA, and the Department of Veterans Affairs (VA) on Payment Integrity in their means-tested programs.[30]

Finally, as shown in Figure 3-2, GAO's July 2015 fraud risk framework has four components, the first of which emphasizes the importance of leadership in the fight against fraud.

> *Commit – Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.*
>
> - *Create an organizational culture to combat fraud at all levels of the agency, [including] demonstrate a senior-level commitment to integrity and combating fraud*
> - *Create a structure with a dedicated entity to lead fraud risk management activities*[31]

Figure 3-2. GAO's Fraud Risk Framework

[30] The accountability community has a parallel effort among the OIGs of these agencies.
[31] A Framework for Managing Fraud Risks in Federal Programs (GAO-15-593SP, July 2015)

3.3 Agencies' Approaches to Root Causes and Corrective Actions

Identifying the true root cause of an improper payment can take time. If the root cause analysis process is short circuited, an apparent root cause (also called a "causal factor") may be identified and mistakenly labeled as the true root cause. An apparent root cause (causal factor) does affect an event's outcome, and removing it can benefit that outcome. However, the true root cause of an improper payment has been identified if removing it prevents the event from recurring.

The "5 Whys" is a technique used in the Analyze phase of the Six Sigma Define, Measure, Analyze, Improve, and Control methodology. By asking the question "Why?" multiple times, the causal factors can be identified and removed, which can lead to the true root cause of a problem. Very often the perceived root cause of a problem turns out to be a causal factor, which leads to asking another "Why?"

Agencies do not always appear to comprehensively dig past the causal factors to the true root causes, and weaknesses in identifying true root causes have led to questions about the likelihood that the related corrective actions will be successful. GAO, for example, has expressed concerns about the overall effectiveness of agencies in fully resolving the root causes of improper payments; some agency officials expressed the same concern. Further, not identifying the true root causes may hinder agencies' ability to discern common cross-government issues, thereby reducing the likelihood that broad strategies will be developed to address systemic root causes.

Agencies are required to annually publish information about their improper payments. Most do this in their Agency Financial Reports (AFR). Analysis of 16 agencies' AFRs for FY 2013 and 2014 showed that while the agencies identified both root causes and corrective actions for their improper payments as required, some of the corrective actions were worded more like additional root causes (causal factors). Agencies often identified root causes that did not seem to have corresponding corrective actions, and corrective actions that did not have "provoking" root causes, raising the question – how thoroughly and effectively are agencies analyzing the root causes and developing the right corrective actions?

For analysis, we placed the agency-identified root causes and corrective actions into a half dozen higher level issue categories such as "Agency Actions" and "Eligibility," as shown in Table 3-1. In linking the root causes and corrective actions, correlation would be expected – i.e., the number of agencies with root causes in a given issue category would equal the number of agencies with corrective actions in that same category, and the number of programs would at least be close (allowing for the possibility of multiple programs having the same general root cause). However, as Table 3-1 shows, in only one issue category did the reported corrective actions correlate to the root causes in terms of number of agencies, and in five of the six categories the number of programs varied significantly. For example, various types of Contract, Grant, and Loan Issues were cited as the root cause of improper payments by 9 agencies in 29 total programs, while 11 agencies showed corrective actions for problematic Contract, Grant, and Loan Issues in 34 programs.

Table 3-1. Root Causes and Corrective Actions by Issue Category[32]

Issue Category	Root Causes	Corrective Actions
Agency Actions	12 agencies, 41 programs	12 agencies, 51 programs
Contract, Grant, and Loan Issues	9 agencies, 29 programs	11 agencies, 34 programs
Eligibility	9 agencies, 24 programs	4 agencies, 7 programs
Errors / Fraud by Applicant or Representative	8 agencies, 37 programs	3 agencies, 6 programs
Medical Provider Actions	2 agencies, 3 programs	None
Outside Agency Control	None	8 agencies, 26 programs

Source: MITRE Analysis of Selected FY 2013 and 2014 AFRs

Overall, the most prevalent identified root cause was Agency Actions (e.g., delays, errors) followed by program Eligibility regarding income level, while the most frequently identified corrective actions focused on improvements in agency processes and training for agency employees and states / grantees / industry.

- Significantly more corrective actions fell in the Agency Actions category than any other, and there were more programs with corrective actions than with root causes in this category, raising the question – do some agencies gravitate to the more easily addressed things (e.g., providing training, revising written procedures, modifying processes) and not enough to effectively identifying and resolving the true root causes?
- The situation was just the reverse for Eligibility and Errors / Fraud by Applicant or Representative – there were more agencies and programs with root causes than with corrective actions. Some agencies seem to have trouble directly addressing the problems at the point where the mistake is made (the applicant or applicant's representative), relying instead on agency processes to catch ineligible applications (i.e., detecting errors during agency processing vs. preventing them or deterring fraud).
- Medical Provider Actions and Outside Agency Control – some agencies and programs had root causes for Medical Provider Actions but no corrective actions, while the reverse was true for Outside Agency Control – corrective actions without root causes (it is possible that problems in some categories, like Eligibility, have to be addressed by legislative changes, but the AFRs often do not state this).

Finally, in analyzing these AFRs, it became apparent that agencies rarely recognized fraud as a root cause of improper payments. When discussing this with agency officials, some admitted that employees need to just admit that fraud can, and does, exist. They indicated that without acknowledging the problem, it is hard to get energized to fight it.

[32] In Table 3-1, some agencies and programs show up in multiple issue categories, and in multiple root causes / corrective actions within the issue categories.

3.4 "Applicant" vs. "Government" Actions Paradigm

The analysis of the AFRs showed that agencies seem, most often, to identify root causes and formulate corrective actions in terms of "government" errors as opposed to "applicant" errors or fraud.[33] This leads to many "catch the agency error" vs. "prevent the applicant error / deter the applicant fraud" corrective actions.

However, it is generally less expensive and less risky to prevent applicant errors and deter applicant fraud than to catch government errors before payment (with processing costs incurred and with the risk that the improper payment will slip through agency controls undetected). This approach can be called "left of check," i.e., the further to the "left" of (before) the issuance of a payment in the overall process (see Figure 3-3), the less expensive and risky. The worst case is to make improper payments and then attempt to recover the funds, an approach often termed "pay & chase," which GAO officials called fundamentally flawed.

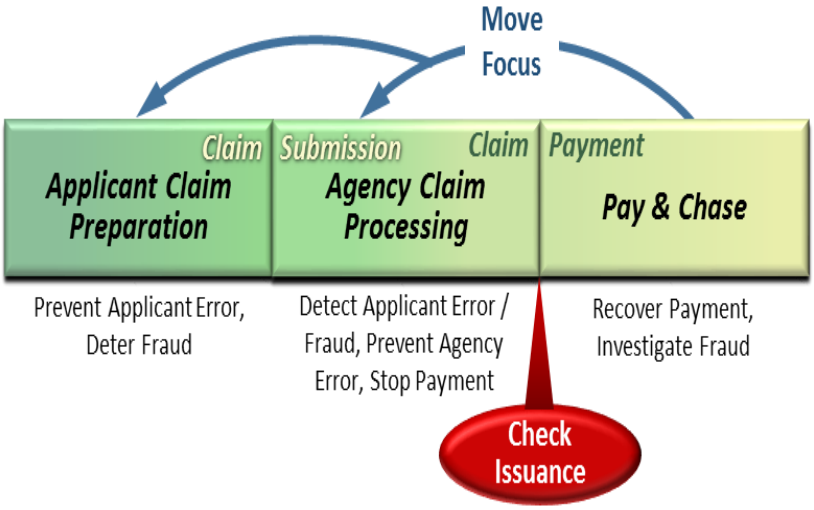


Figure 3-3. "Left of Check" vs. "Pay & Chase"

For example, as previously mentioned, in the healthcare industry between 3 and 10 percent of expenditures are estimated to be lost to fraud, with another 20 percent or more lost to waste (which would include errors) and abuse. Using the more optimistic level of a 3 percent loss of Medicare payouts due to fraud, reported FY 2013 Medicare-related improper payment recoveries that approached $1.8 billion would mean a total recovery rate of only about 10 percent of fraud losses – not an optimal result (see Appendix B for a case study of Medicare and Medicaid). In fact, in its July 2015 fraud risk framework, GAO states that "[P]reventive activities generally offer the most cost-efficient use of resources, since they enable managers to avoid a costly and inefficient 'pay-and-chase' model. Therefore, leading practices for strategically managing fraud risks emphasize risk-based preventive activities."[34]

Best practices for preventing errors and deterring fraud by applicants center on education of, outreach to, and engagement with individuals and groups (e.g., medical associations). Industry experts maintain this is important now, but will be even more so in the future. Agency officials reiterated this, indicating that targeted outreach and messaging to "partner" organizations are

[33] In this usage, "government" includes federal, state and local governments and those acting on government's behalf (grant recipients, healthcare intermediaries, et al). "Recipient" refers to any entity (individuals, organizations, et al) making a claim against the government.

[34] A Framework for Managing Fraud Risks in Federal Programs (GAO-15-593SP, July 2015)

helpful in addressing Payment Integrity to help ensure that they understand, for example, eligibility and reporting requirements. Some agency officials suggested using apps to facilitate widespread communications. Table 3-2 provides examples of outreach and prevention efforts agencies identified as successful in their FY 2013 and 2014 AFRs.

Table 3-2. Examples of Outreach and Prevention Efforts

Practice	Agency	Specifics
Outreach to individuals, practitioners	IRS	• Suite of progressive EITC preparer treatments, addressing over 18,000 preparers selected through a risk-based scoring model: visits, mailings and phone calls to suspect preparers • Warning letters to taxpayers • Public Awareness Days • Working with the tax preparer industry to minimize EITC fraud and errors
	HHS	• Outreach to providers and suppliers – training sessions, individual meetings, presentations at healthcare industry association meetings, dissemination of educational materials, clarification of medical record request letters • Outreach to contractors – monthly meetings to facilitate communication and problem solving • Education task forces develop provider education strategies and materials addressing areas prone to improper payments; hold open door forums to discuss documentation requirements and answer provider and supplier questions; and distribute informational articles as needed to improve documentation and educate providers on Medicare policies • Outreach to TANF participants
Technology enablers	SSA	Automated phone capability and smartphone app to enable SSA recipients to report wage changes
	Depart-ment of Education	Uses the Internal Revenue Service Data Retrieval Tool to enable Title IV student aid applicants and, as needed, parents of applicants to transfer certain tax return information from an IRS website directly to their online Free Application for Federal Student Aid (FAFSA)
Outreach to / working with states	HHS	• Training, technical assistance, support to program integrity officials, newsletters, website for policy / guidance / data / program information, targeted initiatives • State level error rate / improper payment reduction goals, accompanied by measurement, dashboards, etc. • Local office quality control reviews • Training for employees • Establishing and monitoring internal procedures • Grantee Internal Controls Self-Assessment • Peer-to-peer learning
	USDA	• State Exchange Program – sharing info on best practices and effective techniques for error reduction • Partnerships, information exchange, and collaborative efforts that address mutual concerns and support development of effective corrective action
	Depart-ment of Labor (DOL)	National Integrity Summit
Working with contractors	Depart-ment of	• Contract requirements – payment accuracy standards • Business processes for assessing compliance and root causes of inaccuracies

Practice	Agency	Specifics
	Defense (DOD)	
Conse-quences for "problem entities"	IRS	• Issuing return preparer penalties as necessary • Banning some taxpayers from submitting claims for EITC for multiple years

Source: MITRE Analysis of Selected FY 2013 and 2014 AFRs

A variety of research by academicians and MITRE, among others, is ongoing that could provide insights into better ways to identify groups that would benefit the most from education, outreach and engagement. For example, University of Virginia researchers are mining social media for indicators of crimes. MITRE researchers are evaluating social media to identify "chatter" that suggests fraud or misunderstandings that could lead to errors in specific geographic areas; this could be useful in identifying outreach possibilities across specific professions or groups of individuals participating in a certain government benefit program. Other MITRE research could be used to evaluate the effectiveness and impact of targeted communication and outreach to deter fraud or clarify misunderstandings that could lead to errors. Further, recently concluded research has explored a belief-intent framework that could be useful for examining how effective different levers may be in changing the behavior of individuals participating in a specific environment.

3.5 Improper Payments Reporting Categories

GAO has rightly stated that "Analysis of the root causes of improper payments can help agencies target effective corrective actions."[35] This assumes that the correct (true) root causes have been identified.

In 2010 OMB issued guidance in Circular A-123, Appendix C, establishing three reporting categories: documentation and administrative, authentication and medical necessity, and verification. As the guidance was implemented, concerns were raised that because the three categories were general in nature, additional analysis to understand the true root causes was required for agencies to identify and implement effective corrective actions.

In 2014, OMB updated this guidance and expanded the reporting categories to seven. These are a definite improvement over the prior categories, but agencies must still examine the specific issue in detail to understand the true root cause. Further, these categories, like their predecessors, are a mix of true root causes and internal control problems (i.e., apparent root causes). For example, "administrative or process errors [made by] federal agency," which is defined as "[e]rrors caused by incorrect data entry, classifying, or processing or applications or payments," is a true root cause that would directly lead to an improper payment, and if corrected, would prevent the improper payment. "Insufficient documentation to determine," however, which is defined as "[a] situation where there is a lack of supporting documentation necessary to verify the accuracy of a payment…", is an internal control problem that could allow an improper payment to be issued (a causal factor), but it would not actually cause an improper payment to be made (i.e., even without the needed documentation in a case file, the payment may still be completely proper).

[35] IMPROPER PAYMENTS Government-Wide Estimates and Reduction Strategies (GAO-14-737T, July 9, 2014)

This comingling of root causes and internal control problems may lead agencies to identify corrective actions that address causal factors but not true root causes, thereby not resolving the real problems that led to improper payments.

3.6 What Agencies Can, and Cannot, Control

It is usually easier for an organization to solve problems that are under its direct control than those that are not. In the case of improper payments, key aspects of many programs are outside agencies' control, making it more difficult to solve the Payment Integrity problems. In general, as shown in Figure 3-4, agencies may be able to influence Congress, but not control it, regarding how draft legislation might structure a program, or applicants in terms of how accurately they complete a benefit application. Agencies can control their own processing of applications and payments, but can only guide / require and oversee other entities (e.g., states, grantees) that might have key responsibilities in the process. Finally, after payments are made, agencies can control recovery auditing, for example, but have little or no influence over what fraud cases might be prosecuted.

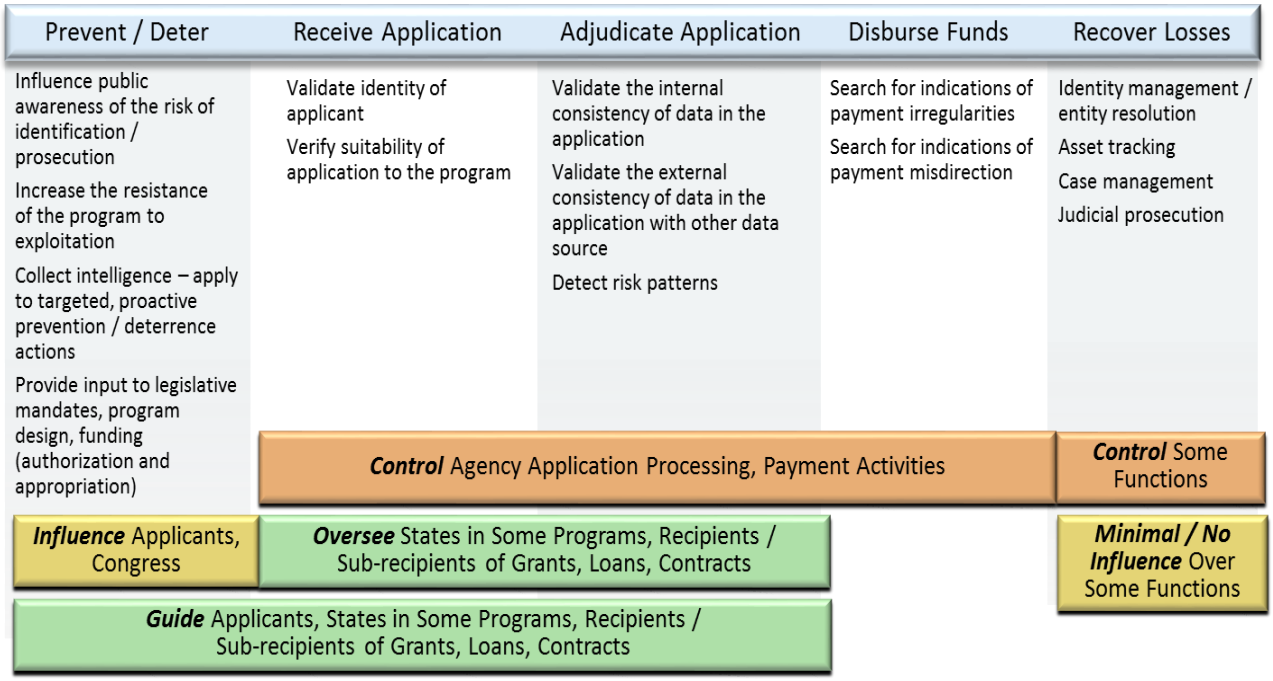


Figure 3-4. Segments of the Payment Integrity Assurance Process that the Federal Government Can Control, Guide / Oversee, or Influence

Agency officials stressed the need to hold the right people and organizations accountable for Payment Integrity. In some cases, for example, agencies do not have insight into what the ultimate recipients, such as sub-grantees, do with the funds they receive. These officials cited the success and value of the visibility provided by the American Recovery and Reinvestment Act of 2009 (P.L. 111–5) at the recipient and sub-recipient levels, and indicated that the same visibility is needed across numerous federal programs.

Agency officials also indicated that ensuring Payment Integrity is sometimes really the responsibility of the states, such as situations in which the program is federally-funded but state-administered (like Medicaid or UI). However, as discussed later in this document, laws and resources available to fight improper payments can vary from one state to the next. Agency officials recognized that gaps and inadequacies in the federal / state relationships need to be

addressed; e.g., cross-state collaboration on some issues would be helpful if statutory prohibitions, state laws, etc., permitted it.

3.7 "Tension" Between Payment Integrity and Making Payments Promptly

Agency officials often described a "tension" between ensuring that payments are proper and getting benefits into the hands of the individuals when they are needed. One well known example cited is the requirement for the IRS to pay refunds within 45 days of the tax return filing due date, which constrains IRS' administration of the EITC program (see Appendix C for a case study of EITC). In other cases, agencies could be putting themselves, or the states, at risk of making improper payments by means of their own internally imposed timeframes that do not allow sufficient time for quality checks / verification.

Accountability officials acknowledged that agencies face a challenge in balancing the need to provide benefits timely with good financial stewardship. Preventing improper payments requires money and time – resources that could be allocated to providing the benefits themselves. But this tension does not need to persist. GAO's July 2015 fraud risk framework states:

Managers may perceive a conflict between their priorities to fulfill the program's mission, such as efficiently disbursing funds or providing services to beneficiaries, and taking actions to safeguard taxpayer dollars from improper use. However, the purpose of proactively managing fraud risks is to facilitate, not hinder, the program's mission and strategic goals by ensuring that taxpayer dollars and government services serve their intended purpose.[36]

In the wake of Hurricane Katrina, for example, GAO pointed out that even in a crushing emergency, fraud prevention and the rapid distribution of assistance are not conflicting mandates; both can be accomplished if effective controls are in place and operating as intended. In cases like the response to Hurricane Katrina, the very nature of the need to quickly provide assistance makes such payments more vulnerable to fraud and error, requiring diligence on the part of relief-providing agencies.

3.8 "Commonalities" and "Convergence" Make Payment Integrity More Challenging and Complex

Two emerging financial crime concepts are particularly relevant to Payment Integrity because they can involve fraud: "commonalities," and "convergence."

"Commonalities" refers to the fact that all financial criminals, at some point:

- Need access to financial institutions
- Need to evade taxes
- Need to launder money
- Seek to move funds off shore
- Have a government agency that oversees them

"Convergence" also is about commonalities in financial crimes. For example, a fraudster will usually store the proceeds of the crime, at least temporarily, in a financial institution of some

[36] A Framework for Managing Fraud Risks in Federal Programs (GAO-15-593SP, July 2015)

kind (bank, money services business, etc.), will likely not report the income on their tax return, and, if the amount is significant, will probably launder the proceeds of the fraud, often internationally. So an initial fraud against one agency expands to include offenses against the agencies overseeing financial institutions, the IRS, and agencies overseeing mortgage lenders or other ways the money may be laundered.

Convergence refers to the need to bring these agencies together with new, more holistic approaches in order to fully address the problem. Private sector organizations of all sizes have embraced the concept of convergence, concluding that many of the separate financial crime control functions and personnel would achieve more as a combined unit than separately. Regardless of exactly how it is done in the federal government, a more holistic approach will enable more effective prevention and detection of fraud and its related financial crimes, since fraudsters count on this vulnerability and exploit it relentlessly.

The concept of convergence is driving private sector organizations towards a "financial crimes risk management" mindset, which includes fraud risk management, with an emphasis on the customer, product, and geographic area involved as being critical to the level of risk. With that in mind, other issues related to financial crime, such as cybersecurity and identity fraud, should also be considered in the overall government approach to financial crimes risk management.

3.9 Conclusions

- The "story" of government Payment Integrity is not being accurately told, which can divert attention from the real solutions needed.
- Ineffective identification of many corrective actions is driven by how agencies approach the problem, which is driven, in part, by the definition of root causes and interpretations of guidance / requirements.
- Inadequate attention being given to fraud minimizes agencies' focus on the need for deterrence and defensive actions.
- Preventing errors and deterring fraud – moving to the "left of check" – are preferable to, and generally more cost-effective and less risky than, "pay & chase."
- The "tension" that exists between making payments on time and making them properly does not need to exist if the right controls are in place and operating effectively.
- Inadequate attention to the full scope of financial crimes that can accompany fraud (commonalities) minimizes agencies' focus on the need for cross-government collaboration (convergence).

3.10 Recommendations

1. Designate a federal executive to chair a leadership group comprised of agency principals to define and oversee a Payment Integrity strategy that addresses government-wide and, as needed, domain-wide issues and to demonstrate a strong "tone at the top."[37] The group's charter would include:

[37] Aspects of this recommendation are also reflected in recommendations the President's Management Advisory Board's Improper Payments Subcommittee made in September 2012: conducting pilot approaches on a set of improper payment challenges to address root causes, establishing new governance and oversight structures for a strong "tone at the top," and tailoring actions based on the highest risk / value opportunities among programs.

- Identifying and prioritizing cross-government initiatives that address significant shared challenges, such as the remaining recommendations in this study
- Involving state and local governments and private partners, when appropriate
- Considering a Cross-Agency Priority Goal for Payment Integrity
- Assessing the potential for a government-wide Payment Integrity Roundtable, which could include not just federal representatives but also state and local governments, private sector, non-profits, and academic institutions

2. Further clarify root cause reporting categories in OMB Circular A-123, Appendix C.
   - Distinguish between what constitutes a true root cause that ***created*** an error vs. an internal control problem (causal factor) that did not ***catch*** an error
   - Using the current OMB reporting categories, frame reporting around:
     - Applicant actions vs. government actions
     - Actual vs. potential losses to the government
   - Specifically segment fraud as a reporting category

Example: Failure to Verify Death Data

Current Reporting	*Recommended Reporting*
Root Cause	Internal Control Problem
Actual Improper Payment	Potential Improper Payment

3. Focus more on preventing errors and deterring fraud than has historically been the case.
   - Expand research on root causes pertaining to applicant errors and fraud
   - Explore corrective actions that could more effectively reduce applicant errors and fraud, such as:
     - Auto populating applications in ways that make errors and fraud more difficult
     - Exploring new outreach mechanisms; e.g., mining social media for indicators of misunderstanding of programs, and then issuing targeted communications to individuals / groups that appear to be outliers in programs
4. Assess existing metrics to determine whether they can better measure the effectiveness of individual agency corrective actions in addressing root causes.

4 Effective Risk Management is Critical, Particularly Relating to Fraud

Risk is an event that, if it occurs, adversely affects an organization's ability to achieve its objectives. Risk management is a formal and disciplined practice for addressing risk and reducing it to an acceptable level. It includes identifying risks, assessing their probabilities and consequences, developing management strategies, and monitoring their state to maintain situational awareness of changes in potential threats. As such, risk management is critical to increasing the likelihood of successful program outcomes.

Risk management can be practiced on an individual project, within a specific program, or across the entire enterprise. The Association for Federal Enterprise Risk Management defines Enterprise Risk Management (ERM) as "a discipline that addresses the full spectrum of an organization's risks, including challenges and opportunities, and integrates them into an enterprise-wide, strategically-aligned portfolio view. ERM contributes to improved decision-making and supports the achievement of an organization's mission, goals, and objectives."

As part of the government's management of improper payment risks, IPERA requires agencies to periodically conduct risk assessments of programs that meet certain defined criteria. OMB Circular A-123, Appendix C provides implementing guidance for this IPERA requirement.

Proactive fraud risk management, in particular, is important to helping organizations understand the fraud risks that can undermine their objectives, determine whether their anti-fraud programs and controls are effective in reducing instances of fraud, and achieve the highest levels of integrity. In fact, GAO's September 2014 *Standards for Internal Control in the Federal Government* requires managers to assess fraud risks as part of their internal control activities.[38] These standards became effective at the start of FY 2016 and are augmented by GAO's July 2015 document, *A Framework for Managing Fraud Risks in Federal Programs*, which "provides comprehensive guidance for conducting these assessments and using the results as part of the development of a robust antifraud strategy."[39] Finally, preventive controls specifically related to Payment Integrity include performing appropriate risk assessments and gap analysis.

4.1 Current Approach Not Fully Facilitating Payment Integrity

The IPERA risk assessment process in general, and fraud risk assessments in particular, should help agencies better understand their Payment Integrity risks and develop mitigations. However, some agency and accountability officials interviewed for the study raised questions about whether the IPERA process provides for addressing all programs that it should and whether it focuses sufficiently on fraud. Others expressed confusion about how to apply OMB's existing guidance and overall approach – is the focus at the enterprise level, or the transaction level, or both? – and asked for a clear vision of the purpose of ERM in regards to improper payments.

Best practices recommend conducting risk assessments at a business unit or program level in a manner whereby the results can be aggregated with other like units or programs, up to and including aggregation at the enterprise level. In the federal government, there are some issues, as previously noted, that are common across domains (e.g., disaster response and recovery) or even

[38] Standards for Internal Control in the Federal Government (GAO-14-704G, September 10, 2014)
[39] A Framework for Managing Fraud Risks in Federal Programs (GAO-15-593SP, July 28, 2015)

across the entire government (e.g., cybersecurity); in such cases, a domain, or the government itself, could be viewed as "the enterprise" for aggregation and assessment purposes (e.g., see the National Terrorist Financing Risk Assessment and the National Money Laundering Risk Assessment). However, the often-found "silo" mentality in agencies or even individual programs within agencies, discussed later in this document, can make aggregating risk assessment results a challenge.

Specifically regarding fraud, as shown in Figure 3-2, GAO's July 2015 fraud risk framework has four components, three of which are to:

> *Assess – Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.*
>
> - *Plan regular fraud risk assessments that are tailored to the program*
> - *Identify and assess risks to determine the program's fraud risk profile*
>
> *Design and Implement – Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.*
>
> - *Determine risk responses and document an antifraud strategy based on the fraud risk profile*
> - *Design and implement specific control activities to prevent and detect fraud*
> - *Develop a plan outlining how the program will respond to identified instances of fraud*
> - *Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy*
>
> *Evaluate and Adapt – Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.*
>
> - *Conduct risk-based monitoring and evaluate all components of the fraud risk management framework*
> - *Monitor and evaluate fraud risk management activities with a focus on measuring outcomes*
> - *Adapt fraud risk management activities and communicate the results of monitoring and evaluations*[40]

Finally, in considering risks across programs, domains, or the entire government, having common risk classifications – a taxonomy – is important for clear communication and understanding, and for effective mitigation. Research in the cybersecurity and financial arenas has shown the value of such taxonomies for assessing threats (risks). However, no such taxonomy appears to exist at any level across the federal government.

4.2 Conclusions

- The current risk management approach limits the government's ability to ensure Payment Integrity.
- Fraud prevention and detection are not always specifically addressed.

[40] A Framework for Managing Fraud Risks in Federal Programs (GAO-15-593SP, July 28, 2015)

4.3 Recommendation

5. Develop a comprehensive and ongoing risk management framework addressing Payment Integrity risks, in particular fraud, based on threat analysis to help agencies better understand their vulnerabilities and better define defenses; include elements such as:
    - Taxonomies for common types of fraud, especially across domains and government-wide
    - Tactics, techniques, and procedures used by fraudsters
    - Attack modalities – ways fraudsters can execute their schemes
    - Fraud risk assessments, in keeping with the GAO's September 2014 *Standards for Internal Control in the Federal Government*[41] and July 2015 document, *A Framework for Managing Fraud Risks in Federal Programs*[42]
    - Consideration of program applicants, benefits / services provided, and geographic areas involved
    - Addressing of risks not just at individual program or agency level, but also domain- and government-wide, and identification of actions needed to mitigate risks at all three levels

[41] Standards for Internal Control in the Federal Government (GAO-14-704G, September 10, 2014)
[42] A Framework for Managing Fraud Risks in Federal Programs (GAO-15-593SP, July 28, 2015)

5 Identity and Eligibility Risks Cut Across Many Agencies

Whether it is for communications involving PII such as an SSN, or for providing services or monetary benefits, federal agencies must assure themselves of the identity of the person or entity with whom they are dealing. Further, agencies need to understand the risks, if any, that the person or entity pose to the program. This is increasingly difficult in an era when identity theft is more and more prevalent.

Eligibility issues also challenge many agencies. Federal benefits programs have numerous and varied eligibility criteria, and ensuring that an applicant meets the specific criteria of an individual program can be troublesome.

The Payment Integrity impacts of both identity and eligibility can be significant. In recent years, IRS, for example, has needed to devote significant efforts to individual tax return processing controls that identify the potential use of false identities in refund fraud. Refundable tax credits are a significant eligibility issue; during 2014 tax filing, IRS estimates that the approximately $18 billion in improper EITC payments went to claimants for whom the IRS could not verify eligibility.

The challenges of identity validation and eligibility verification cut across many programs. They are often similar in their nature from one agency to the next, yet there is currently no capability across government for verifying applicants' identities or eligibility. The broad, but not unique, nature of this challenge suggests consideration of cross-cutting solutions.

5.1 Identity Concerns: Growing and Likely to Continue

Recent incidents of major identity theft such as the OPM data breach serve notice of the massive and increasing scale of the problem. And as previously mentioned, this is a trend that is projected to continue.

Because of this, in recent years important segments of the private sector, such as the financial industry, have instituted preventive controls that feature a customer identification and due diligence program to identify and prevent inappropriate people and entities from becoming customers. Financial Industry Regulatory Authority (FINRA) rule 2090, Know Your Customer, states "Every member[43] shall use reasonable diligence, in regard to the opening and maintenance of every account, to know (and retain) the essential facts concerning every customer…" In general, Know Your Customer (KYC) programs help organizations positively identify potential customers and key information about them before conducting financial business with them. A sound KYC program includes the following attributes.

- Robust account-opening and customer identification procedures that allow the organization to determine the true identity of each potential customer and assess the risk they present. Common account opening procedures and best practices include:
    - Gathering and verifying customer identification materials

[43] The FINRA manual defines the term "member" as "any individual, partnership, corporation or other legal entity admitted to membership in FINRA under the provisions of Articles III and IV of the FINRA By-Laws."

- Validating the customer's identity, including circumstances, business type, and source of funds and wealth, using techniques such as multi-factor authentication
- Screening the customer against sanctions lists, watch lists and politically exposed persons lists
- Documenting the normal and expected activity of each customer, including occupation and business operations

- Anti-corruption compliance activities such as ongoing automated and manual monitoring
- Enhanced Due Diligence for customers that pose a higher risk based on attributes identified at the opening of the account or customer activities after the account is opened
- Employee training and awareness

In recent years some federal agencies have undertaken actions that also hold promise. For example, as mentioned in Recommendation 3, some agencies have begun auto populating selected application forms and electronic records, which can help ensure that applicants complete online forms accurately. However, precautions must be taken because auto populating can inadvertently reveal information to a fraudster who is applying online with just a basic set of identifying information, actually facilitating the submission of fraudulent claims.

In another example regarding disaster assistance in the wake of Hurricane Sandy, GAO reported in 2014 that the Federal Emergency Management Agency (FEMA) used a tool to validate the identity of applicants during registration. FEMA also hired contractors to inspect damaged homes to verify the identity and residency of applicants and to confirm that reported damage was a result of Hurricane Sandy. However, GAO reviewed SSA data that FEMA does not use, such as SSA's most complete death records, and found 2,610 recipients with potentially invalid identifying information who received $21 million of payments that may have been improper. GAO suggested that collaborating with SSA prior to providing assistance could give FEMA additional information to further reduce its risk of assisting ineligible applicants.[44]

5.2 Agencies Need Data to Verify Eligibility

Determining eligibility is complicated by a number of factors, some of which (discussed later in this document) are the following.

- Definitional issues in legislation can confuse applicants and make eligibility determination difficult for agencies.
- Legislative requirements for such things as the timing of payments can hinder agencies' ability to verify eligibility before making the payments.
- Program design (whether legislatively mandated or agency-established) can force agencies to rely heavily on self-reporting by benefit recipients, especially for "life changes." For example, a person can be eligible for a program when they initially apply, and then 6 months later a change in their life circumstances (such as getting a higher-paying job) should cause them to lose eligibility; improper payments may result if the person does not self-report the change.

[44] HURRICANE SANDY FEMA Has Improved Disaster Aid Verification but Could Act to Further Limit Improper Assistance (GAO-15-15, December 12, 2014)

A significant concern that agency and accountability officials consistently reported was the availability of the data needed – at all, or when needed – to verify eligibility. In some cases, data does not exist to allow agencies to independently verify eligibility. In other cases, the data is available but agencies are prohibited from using it (such as IRS tax-related income data) or do not have matching agreements in place to take advantage of it. Finally, there are situations where the data exists and can be matched, but problems exist with the data.

- It may not be available until after the payment is required to be made; even when self-reporting is relied upon, having data at some point in the future to verify eligibility is helpful.
- There may be data quality issues; for example, marriage or death data reported to the federal government from a variety of sources may not be accurate or complete.

Some federal data sharing best practices exist to help with eligibility determination. CMS, for example, has established a federal data hub to allow itself and the states to access a variety of data sources from IRS, the Department of Homeland Security (DHS), SSA, VA, DOD TriCare, and OPM to help with determining eligibility. The data hub routes a user to these other sources instead of pulling in data from them. Further, GAO's 2014 report regarding disaster assistance in the wake of Hurricane Sandy pointed out the following.

FEMA was unable to identify potentially duplicative rental-assistance payments to recipients of its Sheltering and Temporary Essential Power pilot program, in part because it did not request the necessary data from states at the program's outset. FEMA [then] took steps to make data sharing among programs easier, including initiating a committee to explore ways to maintain and share relevant data needed to evaluate and help prevent potentially duplicative assistance…[45]

However, when data sharing opportunities are not pursued, opportunities to prevent improper payments can be missed. In the same 2014 report, GAO stated:

…FEMA relies on self-reported data from applicants regarding private home insurance – a factor the agency uses in determining benefits, as federal law prohibits FEMA from providing assistance for damage covered by private insurance. By examining data from entities that provide federally backed mortgages, GAO identified 534 individuals receiving over $2.3 million in home repair and personal property assistance who said they did not have private insurance but had mortgages that require such insurance…[indicating there is a] risk…that some individuals may have received assistance from FEMA for ineligible expenses.[46]

Eligibility problems are not new. A 2007 MITRE survey found that benefit eligibility determination processes was an area where the least progress had been made in recent years and that, while technology could help address parts of the problem, other non-technical challenges would still remain. MITRE concluded the following (these issues are further discussed later in this document).

- Many issues existed related to the collection and validation of a core set of data elements critical to determining eligibility across multiple programs. In particular, similar terms had different definitions across programs, making it difficult to share data; for example,

[45] HURRICANE SANDY FEMA Has Improved Disaster Aid Verification but Could Act to Further Limit Improper Assistance (GAO-15-15, December 12, 2014)
[46] HURRICANE SANDY FEMA Has Improved Disaster Aid Verification but Could Act to Further Limit Improper Assistance (GAO-15-15, December 12, 2014)

the Public Housing Assistance program defined a "household" as people who live together, while SNAP defined a "household" as people who prepare meals together. In addition, cross-state validation was hampered because of state-specific databases and, for some programs, state-specific eligibility rules. Further, it was difficult to find accurate and timely sources of data to use in validating information that changes frequently (e.g., income, assets, relationships, and work status).

- Existing statutes, regulations, procedures, and funding sources constrained efforts and / or did not provide the leverage needed to reduce improper payments.

5.3 Ongoing Research

MITRE has a wide array of research ongoing which would be useful in formulating solutions to the government's identity challenges. This research ranges from an Identity Matching Lab to internally-funded projects on specific identity issues, such as:

- Identification of key attributes such as gender and age
  - "Properties" of people who are representing themselves to be a certain person
  - Keystroke dynamics
  - "Signatures" on digital devices
- Online identification – "internet persona" vs. real human identity
- Confirmation of identities across multiple datasets

Likewise, MITRE has been conducting internally-funded research to identify ways for the government to better establish applicant eligibility.

5.4 Conclusions

- Identity issues (theft, validation) challenge many government programs as well as the private sector.
- A variety of legislatively defined eligibility requirements impede agencies' ability to cost-effectively make eligibility determinations.
- Lack of data sharing impedes agencies' ability to make eligibility determinations.
- Government reliance on self-reporting is inadequate for thorough verification of eligibility.
- Most, if not all, issues present when MITRE did an initial study of means-tested programs eligibility issues in 2007 are still present today; many go back decades (e.g., UI issues can be traced back to the original legislation in the 1930s).

5.5 Recommendations

6. Assess specific risks presented by the use of false (stolen, synthetic) identities.
7. Incorporate selected aspects of private sector KYC programs in agencies' identity validation processes, such as:
   - Establishing, and then analyzing against, expected behaviors
   - Screening against watch ("gray") lists

8. Reduce reliance on self-reporting by benefit recipients where it causes the most risks; for example:
   - For affected programs, make needed data available via legislative or program design changes, or acknowledge that some improper payments cannot be prevented
   - Require federal program applicants to grant permission, when applying, for necessary validation of financial and other eligibility information with appropriate data sources
9. Identify and pilot test agency-specific and government-wide alternatives for making identity and eligibility determination processes more rigorous, data driven, and cost-effective; for example:
   - Develop a shared service for identity and / or eligibility determinations domain- or government-wide
   - Develop a single point of entry to all federal programs, allowing identity validation, eligibility verification and information sharing across programs (drawing from existing data sources), and giving the user the ability to see all federal programs for which they may be eligible; this would:
     - Reduce fraud with state-of-the-art identity validation
     - Reduce errors and fraud with complete, timely eligibility verification
     - Help the underserved know what they are eligible for and assist them with applying

6 Analytics Hold Great Promise, but Important Challenges Must Be Overcome

Data analytics are an integral part of a robust set of control activities to prevent and detect fraud and other improper payments. These activities include controls that are designed to deter fraud and prevent errors before they occur – well to the "left of check" – and then detect them as early as possible if they do, in fact, occur. GAO has stated that:

[P]reventive controls can help screen out the majority of fraud, and are the most effective and efficient means to minimize fraud, waste, and abuse. They are most effective when they require validation of data provided by [program applicants] against other government or third-party sources, and physical inspections when…possible. Preventive controls…include procedures designed to identify problem [applicants] prior to payments.[47]

Detection, monitoring, and aggressive prosecution of individuals committing fraud – while also crucial elements of an effective system – are less effective and generally cost more than preventing the payments in the first place. Detective controls include:

- Identifying suspicious activity through referrals by employees, automated transaction monitoring, and other customer or transactional monitoring tools and processes
- Monitoring customer activity
- Applying predictive analytics for customer-centric, cross-channel fraud detection
- Screening, blocking and rejecting transactions and customers appropriately

While analytics are critical to keeping up with ever-changing fraud schemes, the real key to achieving success with analytics is not so much the specific approach or tool used, but rather the ***data***, in particular determining which features in the data to leverage. Further, having ***what*** data is needed (including sharing data among agencies and having access to all needed commercial and open source data sets), ***when*** it is needed, at the level of ***quality*** that is needed, are all critical for successful analytics, but as discussed below, are often major challenges for agencies.

6.1 Significant Ongoing Analytics Activities

A number of significant analytics efforts are ongoing at the federal level and at the state level for federally funded, state-administered programs. While there is no "one size fits all" approach, centralizing analytics has shown to be helpful in identifying important patterns of problems. As such, the President's FY 2016 budget includes funding requests for selected program integrity efforts aimed at reducing improper payments, such as:

- CMS' Fraud Prevention System, a state-of-the-art predictive analytics technology to identify and prevent Medicare fraud, along with the CMS Center for Program Integrity and the Healthcare Fraud Prevention Partnership

[47] INDIVIDUAL DISASTER ASSISTANCE PROGRAMS Framework for Fraud Prevention, Detection, and Prosecution (GAO-06-954T, July 12, 2006)

- DOL's UI Integrity Center of Excellence – a federal partnership with state governments to facilitate the development and implementation of UI integrity tools by the states and to share best practices in the detection and reduction of improper payments
- Treasury's DNP solution

6.2 Analytic Approaches and Tools are Critical

To effectively combat improper payments, federal agencies need a capability to identify questionable individuals and transactions at a granular level, a "synthesizing capability" to enable making sense out of disparate data, and the ability to perform strong trend analysis at a bigger picture level. The sheer numbers of entities (individuals, businesses) and transactions, and the costs involved, makes the use of technology, in particular analytic tools, essential. In fact, a 2013 SAS / UBM Tech survey found that federal, state, and local government respondents consistently cited three top drivers for using fraud prevention and detection technology:

- Dealing with new types of threats that current processes are not effectively handling (47 percent of federal respondents and 46 percent of state / local respondents)
- Reducing the cost of combating improper payments (42 percent of federal respondents and 48 percent of state / local respondents)
- Predicting the likelihood of fraudulent events or behavior (33 percent of federal respondents and 43 percent of state / local respondents)

Some experts maintain that without automation, organizations will never be able to catch up with the ever changing tactics of fraudsters. As such, analytics represent an accelerator of capabilities, allowing organizations to correlate, uncover, and predict emerging behaviors much faster than any other way.

6.2.1 Private Sector

A wide array of commercial technology and methodologies exist to help fight improper payments. Numerous product vendors and consulting service companies have a significant presence in the Payment Integrity space, marketing solutions and services to both federal agencies and specific private industries such as financial services. In fact, in the financial services industry alone, well over 70 commercial software tools – some very broad in their focus, some very narrow – and data sets are available to help detect indicators of potentially fraudulent transactions and to assist in critical activities like identity validation. For example:

- One firm's tools focus analytics on high-speed, real- / near-real-time analytics after transaction processing but before payment. The tools feature self-adaptive predictive analytics, link and social network analysis, dashboards, and ad hoc query capabilities. A key feature of their approach is an emphasis on the ability to normalize data from multiple data sets.
- Another firm is conducting extensive research with identity issues. They have a particular interest in supply chain and procurement fraud, and have compiled significant financial data that could help ensure Payment Integrity in those areas.
- Yet another firm is focused on the increasing complexity of rules based analytics, anomaly detection, and predictive models.

Beyond commercial firms, certain private sector entities are recognized as thought leaders because of their advanced defenses against fraud. Some insurance companies are known for particular areas of expertise, such as several disability insurers with the use of models and a number of payers with rule-based approaches. Certain firms in the financial industry that issue credit cards have strong anti-fraud approaches.

While competing firms promote the capabilities of their tools and methodologies, some industry experts maintain that "the perfect solution is not out there," citing the nature of various domains like healthcare or financial services as being so complex with too many variables on transactions that have to be collected and analyzed. Other experts suggested that all of the tools available are essentially comparable, maintaining that the real keys to achieving success with analytics are such things as:

- Determining which features in the data to leverage
- Ensuring the data is of sufficient quality
- Achieving a high level of cooperation between organizations to foster sharing of data
- Ensuring the investigators, regulators, subject matter experts, data scientists, et al, working on an organization's Payment Integrity problems have the requisite knowledge and skill sets

6.2.2 Federal Government

In discussing analytic approaches currently in use, lessons learned to date, and more, agency officials described the following considerations and priorities for data analysts and analytic tools.

- Let customers' needs significantly drive the analytics and tools used
- Ensure multiple data sets can be used ("federated") across multiple tools
- Effectively integrate and normalize disparate data
- Control access to data across geographic boundaries
- Move from summaries of data to higher level modeling that can provide insights of greater value from data
- Quickly identify and characterize high value information
- When choosing an analytic tool:
    - Clearly define the mission a tool must accomplish; do not start the process with "This is the tool I [the analyst] need," but rather "This is the analytic problem I need to solve"
    - Consider the type of data being analyzed and the level of skill and knowledge of the analysts who will use the tool
    - Ensure users can quickly learn how to use a tool without the time and cost of week-long training classes
- Use ad hoc, short term analytic cells to solve problems, with the team members returning to their own organizations – in essence "learning how to fish" and then moving on to share the knowledge and approaches learned with others in their organizations
- Use an agile approach to dramatically shorten analytic solution delivery timelines

- Be open to moving to the cloud which could open up new analytic possibilities with additional data sources that will be available (while maintaining a focus on security)

Some agencies highlighted successful analytic best practices in their FY 2013 and 2014 AFRs, as shown in Table 6-1.

Table 6-1. Selected Agency Best Practices as Presented in FY 2013 and 2014 AFRs

Practice	Agency	Specifics
Automated edit / logic / "red flag" checks during claim processing	IRS	• Identifying tax returns for examination and, in the majority of cases, holding the EITC portion of the refund until an examination can be conducted; also holding the Additional Child Tax Credit portion of the refund on these EITC examinations (this is the only ongoing IRS program where examinations are conducted before a refund is released) • Using fraud detection filters during return processing (EITC)
	SSA	Using logic checks in SSA processing systems
	DOD	A Business Activity Monitoring Tool identifies and prevents improper payments in the 5 largest commercial payment systems
Data matching / verification with third-party data	IRS	Document Matching: Comparing income information provided by the taxpayer with matching information (e.g., Forms W-2 and 1099) from employers and other third parties to identify discrepancies
	HHS	Working with state Medicaid data in the Medicare-Medicaid Data Match program
	SSA	Verifying information using third-party sources
	DOD	Validating existence of DOD retirees / annuitants, especially if over a certain age
	DOL	UI – matching with National Directory of New Hires, state directories of new hires, state wage records, DHS's Systematic Alien Verification for Entitlement system, prison records, state databases with claimant contact information, state unemployment tax data, and other data sets
	Education	Enhancing verification procedures, e.g., requiring selected schools to verify specific information reported on the FAFSA by student aid applicants
Modeling	SSA	Using a predictive model for disability

Source: MITRE Analysis of Selected FY 2013 and 2014 AFRs

Agency and accountability officials cited a number of additional points that would strengthen analytics across government.

- Predictive analytics can be helpful in prioritizing cases, identifying new ones, and improving controls, especially by creating a learning system.
- Cross-agency data sharing is needed, even with data sets that agencies collect for their own purposes (e.g., SSA's Death Master File [DMF]); this would be in addition to, not in place of, something like Treasury's DNP solution.
- "Outside the box" thinking is needed in terms of data sets that could be used to strengthen analytics, for example, beyond the limited number of data sets legislatively mandated for the DNP solution.
- A centralized analytics and data sharing capability should be created.

- Commercial and financial institutions' data sets should be used for validation and verification.
- States need to share data more effectively, especially with major programs like Medicaid and UI.
- States need to better collect eligibility information and provide it more timely.
- Programs need to rely on data more and self-reporting less.
- Visualization / reporting needs to facilitate understanding of the big picture and trends, not just anomalies with individual transactions.

6.3 A Number of Issues Challenge the Federal Government with Analytics

6.3.1 Organizations Rely Significantly on Tips vs. Analytics

Both public and private sector organizations continue to rely heavily on tips for the initial detection of fraudulent activity. The Association of Certified Fraud Examiners' 2014 study[48] reported that in each of its biennial surveys going back to 2010, over 40 percent of frauds had been initially detected by tips. Another roughly 29 percent were detected by management review and internal audit. Controls such as account reconciliation, surveillance and monitoring, and information technology (IT) controls identified only approximately 15 percent.

One reason for this can be false positives from some analytics that stress organizational capacity to verify and process result sets. Another reason can be limited data – i.e., an organization may have minimal history with identifying actual fraud and not enough data to use advanced analytical tools to lower false positive rates to acceptable levels. Despite these occasional shortcomings of analytic approaches, agencies are ultimately better off using analytics than human means alone; what is important is building the data resources to allow the analytical tools to be effective.

6.3.2 Human Capital Issues

No matter how user-friendly tools and methodologies may be, skilled humans are still needed to direct their efforts and to interpret their results. In particular, human judgment is required to understand the context and successfully direct the tools to identify potential improper payments. Domain and statistics experts are needed, as well as experts to regularly update the configuration of a tool, monitor its modeling of the environment, and interpret its output within the context of the changing domain and threats. These skillsets are in high demand, and as discussed previously, the current and predicted future supply is limited.

6.3.3 Analytic Environment Changing Rapidly, but Agencies Not Always Funded to Keep Up

New tools, approaches, and commercial data sets frequently appear that could help agencies combat fraud and other improper payments, and with marketplace competition, many of these tools are becoming more economical. However, funding challenges often constrain agencies'

[48] Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study (Association of Certified Fraud Examiners, 2014)

ability to take advantage of them. This occurs at both the federal and, particularly, the state / local levels.

Fraudsters learn, over time with experience, what types of transactions will get flagged as potentially improper, so it is advantageous to make investments periodically to upgrade or change tools or approaches. The public, however, especially fraudsters, may suspect agencies' limited funding could provide opportunities for successfully submitting questionable claims or for outright fraud.

6.3.4 Pre-pay Analytics: More Cost-effective than Post-pay but Harder to Cost-justify

Some experts indicated that the analytics environment is fast changing between pre-pay (before the payment is issued) and post-pay (after the payment is issued) analytics. In one major industry, years ago the emphasis was strictly on post-pay analytics. Then over time it shifted to pre-pay analytics. However, pre-pay analytics declined again because it was very difficult to demonstrate a return on investment (ROI) that satisfied management, largely due to the fact that there was not enough capacity to understand the overwhelming number of possible variances combined with what is, and is not, acceptable in a claim. As a result, they predominantly use post-pay reviews now, but would prefer using more effective, ROI-sufficient pre-pay tools.

Other experts indicated they perform both pre-pay and post-pay analytics, stating that designing effective pre-pay analytics depends on the quality of the staff. Knowledgeable staff are allowed some freedom to take initiative – e.g., reviewing literature in the domain to identify improper payment issues other organizations were confronting that might also impact their organization, and then structuring analytics to see if their data reveals the presence of the same issues.

In both situations, the experts highlighted the greater value of pre-pay analytics. This would include analytics that could prevent errors or deter fraud in the first place, keeping "bad" claims from ever entering the organization's processing system. The challenge is to be able to demonstrate adequate ROI the further "left of check" that analytics, and preventive controls in general, are incorporated.

6.3.5 Regardless of Tools and Methodologies, Data Can be a Problem

Having ***what*** data is needed, ***when*** it is needed (i.e., "fit for purpose"), is quite often a major challenge in the fight against improper payments. In many cases the data agencies need, e.g., to verify eligibility, either does not exist or is not available to them. Examples include the following.

- "Income level" is a commonly found criterion of eligibility for means-tested benefits programs, but not all programs have access to IRS income data because of legislative restrictions. In some cases, like the SSI program (discussed elsewhere in this document and in a case study in Appendix D), the IRS data is available but not at the time needed.
- The Hurricane Sandy supplemental appropriation did not contain a mandate that agencies give the Program Management Office (PMO) at HUD the data needed to monitor where the money went in order to help ensure Payment Integrity. So the PMO had to rely on establishing trust that they would keep the data secure in order to convince the other agencies to share their data.
- Data is not always of sufficient quality – accurate, complete, and current. Time and money are usually needed to cleanse data before analytics can be performed.

Anecdotally, 80 percent of the effort and resources needed for an effective analytics solution implementation is spent organizing and cleansing data so that it can be analyzed.

- Some data compiled by one agency for its own use are later discovered to be needed by other agencies, but the data may not contain everything that the other agencies need, or it may not be in the same format. SSA's DMF is an example. SSA created and maintains it for their purposes, but over time other agencies have found it to be useful. However, some of those agencies express concerns about the currency of the data or its format, and SSA does not have the funding to make changes solely for the benefit of other agencies, especially when the DMF meets their needs. Despite that, accountability officials believe more agencies need access to DMF.
- Some federal needs for electronic data from states are not met because the states submit hard copy or scanned (non-computer readable) images to federal agencies.
- Some agencies ineffectively manage key data, e.g., spreading it among multiple systems thereby making it difficult to compile and make available to other agencies.
- Very elaborate data sharing solutions may not work due to complexity or cost; in some situations addressing 80 percent of the problem space, vs. trying to address everything, may be the best approach.
- Scaling "local" data sharing solutions to a larger community (e.g., from one agency program to domain-wide or government-wide) can be challenging when the initial solution was developed for a narrow problem. This can be due to cultural issues (e.g., an agency focusing strictly on its own program when it is known to be part of a larger domain with common issues that lend themselves to systemic solutions) or technology issues (e.g., interoperability), both discussed later in this document.

There are some success stories when agencies and states work together to make needed data available. HHS reported the following in its FY 2014 AFR.

The Public Assistance Reporting Information System (PARIS) is a federal / state partnership with all 50 states, the District of Columbia, and Puerto Rico that provides state public assistance agencies detailed information and data to maintain program integrity and detect and deter improper payments in TANF, Medicaid, Workers' Compensation, Child Care, and…SNAP. HHS, the…VA, and…DOD partnered to advance the PARIS project at no cost to states. DOD… provides computer resources to produce a match file, using Social Security numbers submitted by the states, VA, and DOD as the key match indicator. States verify the matched individual's eligibility and take any necessary action. HHS contributes to this effort by executing Computer Matching Agreements and coordinating the quarterly matches. Since its establishment, PARIS has strengthened program administration among its programs and state public assistance agencies. For instance, three states reported that PARIS led to reported savings or cost avoidance of approximately $93.4 million in FY 2014 alone.

6.4 Communication and Information Sharing are Important

Ongoing communication and information sharing among agencies can be critical to combatting common threats. This need gained widespread recognition years ago in the Intelligence and Law Enforcement Communities. Examples like the Joint Terrorism Task Force and the Cybersecurity Roundtable, along with the advent of small cell analytic approaches, have shown value in quickly addressing threats. Similar concepts under

the umbrella of Information Sharing and Analysis Centers (ISAC) are at work in the cyber and critical infrastructure domains; the aviation industry has the Federal Aviation Administration's Aviation Safety Information Analysis and Sharing center; and IRS recently announced an ISAC to combat tax-related identity theft.

Many agency and accountability officials, as well as private sector experts, expressed the belief that having such an operation at the federal level to help ensure Payment Integrity is needed. Timely communication and information sharing about issues, threats, and fraud schemes would be critical in addressing them before significant loss occurs. One private sector expert indicated that hearing speeches at conferences about topics of concern means those problems are already a year or two old, and that if successful ISACs could be set up at the federal level for key domains, it could make a "huge difference" and put the Payment Integrity community "light years ahead" of where they are now.

One aspect of this process could be reporting systems analogous to the existing Suspicious Activity Reports (SAR) and Currency Transaction Reports filed by financial institutions and money services businesses. In some domains, "human sensors" work every day with claims of various kinds, e.g., those who support medical coding operations, and are likely to recognize anomalous transactions in the regular course of their work. The overall Payment Integrity system might benefit from having suspicious activity reporting systems for these "human sensors." While there are limits on agencies' resources to analyze and respond to these reports, there are also approaches in the Intelligence Community that could be leveraged to maximize their potential.

6.4.1 Maturity Models Generally Not Applied

Capability maturity assessment models can help agencies better understand the strengths and weaknesses of some of their risk mitigation actions, such as the use of data analytics in addressing Payment Integrity risks. These models serve to point out where an agency's current operations stand against the array of possibilities, in order to identify additional capabilities that may be valuable to obtain. They can also enable agencies to compare themselves to one another in order to learn about strengths and best practices. However, there does not appear to be an accepted, standard data analytics capability maturity model in use across government. One such private sector model can show an agency how to move from very basic paper reporting of possible fraud to predicting and stopping fraud before it happens – a pathway of increasing complexity leading to improved Payment Integrity outcomes.

6.5 Ongoing Research

As previously discussed, a number of trends are expected to continue, while unanticipated ones may join the picture, all of which could exacerbate government Payment Integrity challenges. While models may be used to address individual issues, none were identified that are designed to specifically predict potential Payment Integrity problems. MITRE has conducted research in quantitative demand forecasting that could be applied to identify and quantify drivers in demand to help predict potential Payment Integrity problems. This MITRE research performed exploratory analysis of the statistical relationships between potential drivers and improper payment levels. With further analysis, these statistical relationships could be used to inform scenario-based projections of improper payments for high risk programs.

As an analogy, MITRE prototyped a System Dynamics model of VA housing programs to quantify the impact of budget changes on the progression of Veterans out of homelessness and into permanent or independent housing. A System Dynamics approach was used because:

- The Ending Veterans Homelessness program is a major transformation with many disruptive elements.
- There is uncertainty regarding the impact of program decisions on the homeless population.
- Complex feedback is involved; transitional programs provide a path out of homelessness where Veterans remain at risk, while prevention reduces the rate of new homelessness.
- System Dynamics provides a tool for understanding the larger pattern of behavior that unfolds over time, allowing VA decision makers to assess the implications of various funding scenarios on the Veteran homeless population.
- The System Dynamics approach allows important causality to be taken into consideration.

6.6 Conclusions

- Agencies need the right data – mature data – at the right time to perform effective pre-pay analytics.
- Funding and skill set challenges limit analytics that some agencies are able to perform.
- Agencies may not understand the full potential for analytics to address Payment Integrity challenges – individually, across domains, and government-wide.
- Tools and methodologies are important, but even more critical is the data itself.
- Technology or data analytics should not be thought of as "the" solution, but rather as "part of" the solution, along with broader, more strategic approaches.

6.7 Recommendations

10. Establish a shared, government-wide research and data analytics capability to enhance prevention and detection of improper payments – a Payment Integrity Research and Analysis Capability (PIRAC);[49] considerations include the following (see Figure 6-1, Figure 6-2, and Figure 6-3 for conceptual examples):
    - Evaluating alternatives for predictive and prescriptive modeling of future trends and their potential impacts on Payment Integrity to serve as an "early warning system" to help inform planning and prevention activities
    - Building a dedicated team of fraud prevention and detection specialists – drawn from agencies and outside organizations
    - Establishing cross-agency / domain-wide work groups to share best practices and performance information and to collaborate on solving systemic improper payments problems (e.g., analytic cell approach)
    - Establishing a governance approach

[49] Aspects of this recommendation are also reflected in recommendations the President's Management Advisory Board's Improper Payments Subcommittee made in September 2012: centralizing data and using real time analytics, and dedicating a team of internal and external specialists to fraud prevention and detection activities.

- Architecting a secure, flexible, agile environment able to respond to advances in analytics tools, methodologies and the varying needs of agencies, with attention to:
  - Multi-tenancy architecture
  - Service level offerings
- Developing and implementing analytics approaches that can start small and then scale to larger applications as capabilities evolve (e.g., individual agency to domain-wide, to government-wide)
  - From information and data sharing…
  - To cross-government analytics…
  - To a federated / hub-and-spoke model as a cross-government partnership
- Establishing mechanisms and methodologies to address data access and sharing issues
- Prioritizing challenges to be addressed based on appropriate mission and ROI considerations
- Developing a communications mechanism similar to the near-real-time efforts of the Joint Terrorism Task Force and ISACs to provide:
  - Actionable information about threats
  - Information about best practices in preventive and detective controls, e.g., advanced edit checks
  - A mechanism for SAR-like reporting in appropriate domains
- Factoring in the relationship / interaction with the Treasury DNP solution

11. Establish an analytic capability maturity model for agencies to use in assessing their analytic capabilities and for identifying needed improvements.
12. Assess existing metrics to determine whether there are better ways to measure the ROI for pre-pay analytics.

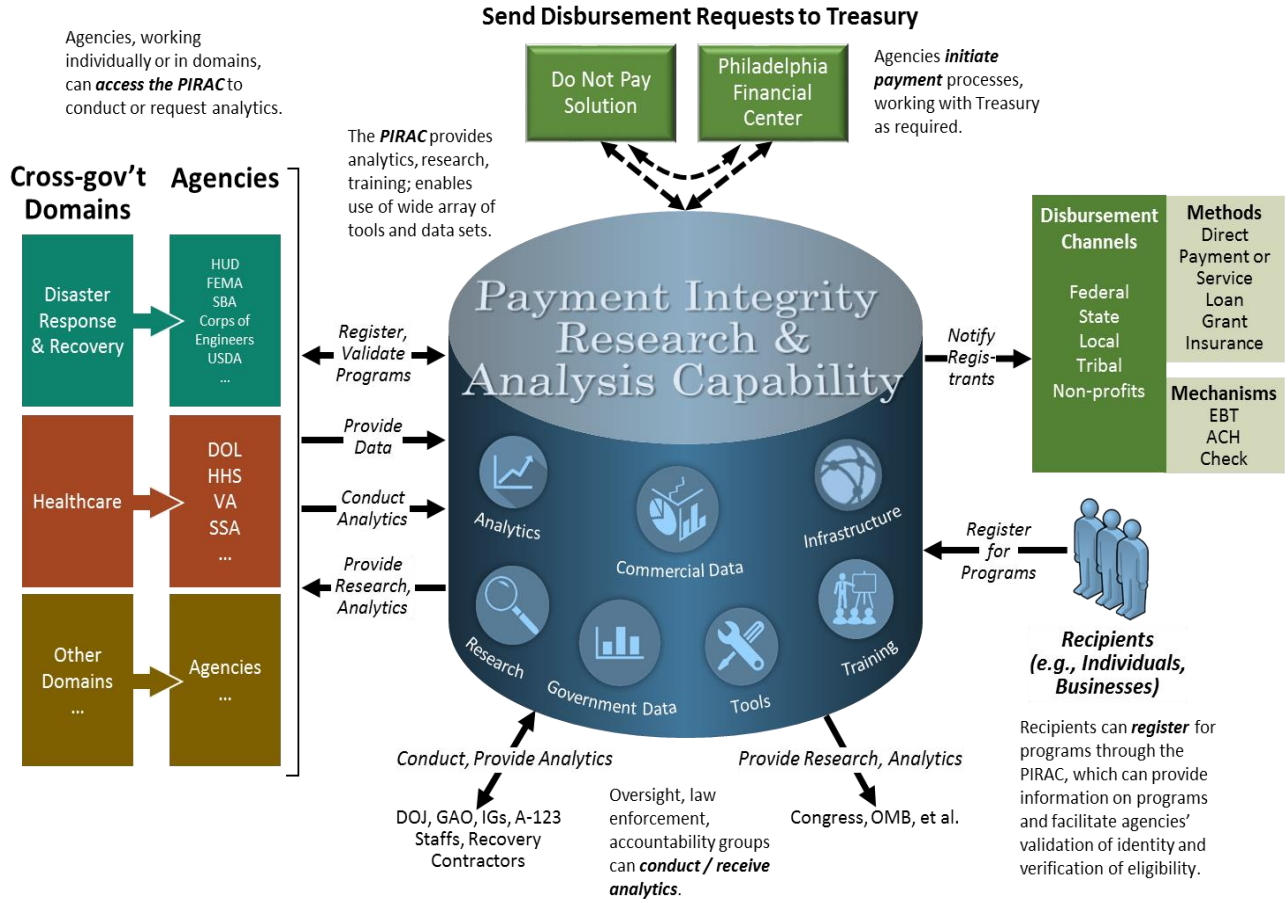


Figure 6-1. Shared, Government-wide Research and Data Analytics Capability: Conceptual Model

Governance body oversees operation of the PIRAC.

Agencies access PIRAC through established Work Groups that could be agency- or domain-specific. Work Groups contain:

- SMEs from one or multiple agencies and elsewhere based on research problem / questions
- Personnel familiar with the type of analysis needed and the data needed to perform the analysis; can come from agency / FFRDC / academia / vendor
- IT personnel from the agency who know about the agency data

Access is via secure portals.

The ***PIRAC*** provides the operating infrastructure, analytic tools, and data sets. Agency data can be stored in the PIRAC or ingested from agency systems for specific analytics. Commercial data would be stored in the PIRAC.

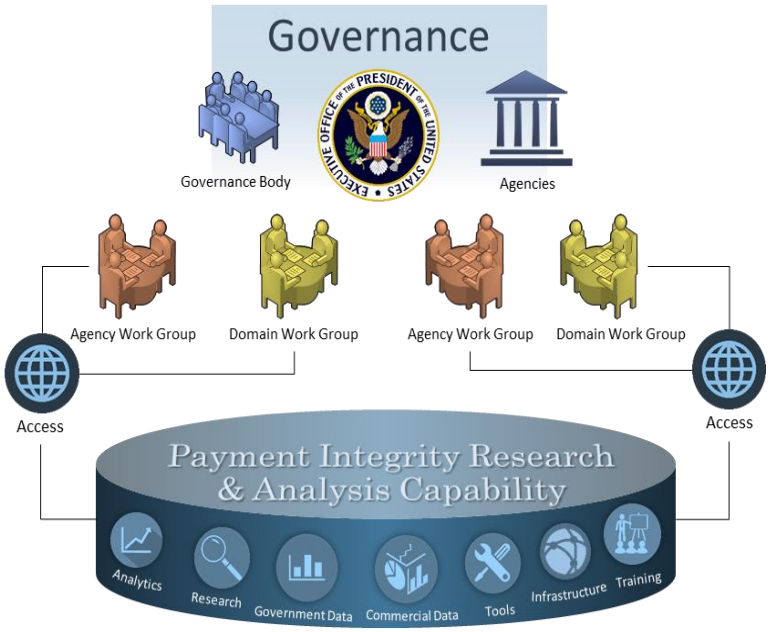


Figure 6-2. Shared, Government-wide Research and Data Analytics Capability: Conceptual High-Level Operation

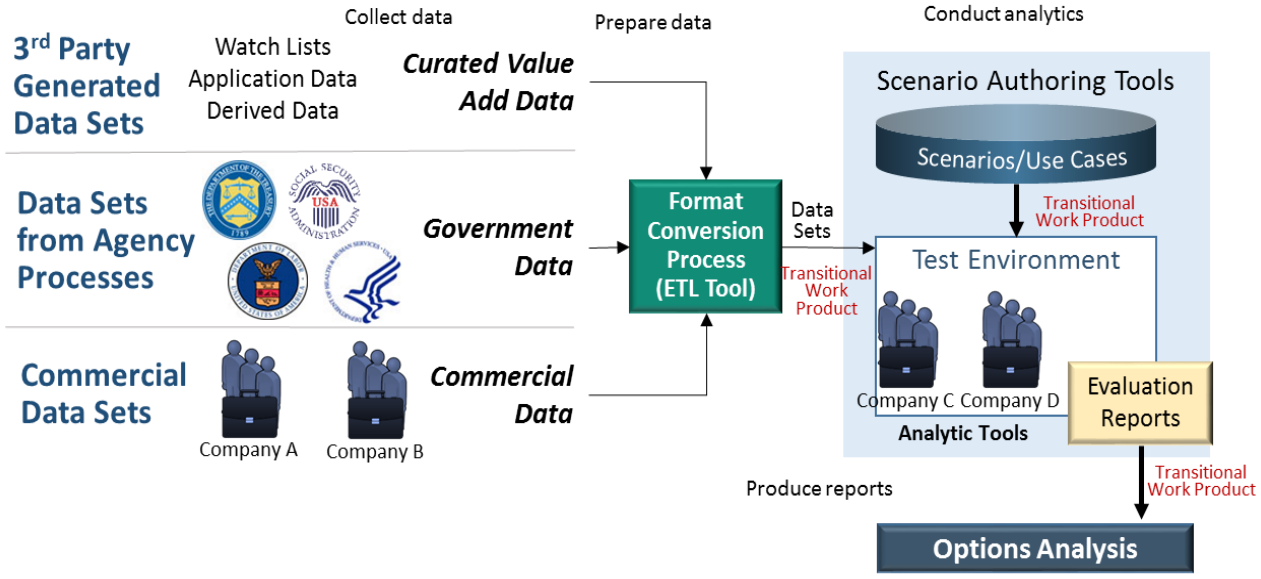


Figure 6-3. Shared, Government-wide Research and Data Analytics Capability: Conceptual Detailed Operation

7 Some Legislation Presents Barriers and Obstacles to Payment Integrity

Certain statutes present challenges to Payment Integrity. Some create or exacerbate the potential for improper payments, while others hinder agencies' ability to resolve Payment Integrity problems. Some accountability officials, in particular, indicated these challenges create a significant concern in that agencies, in general, do not have access to all the useful and relevant data that they need for matching purposes, citing two particular examples.

- They maintained that only agencies that provide benefits have access to the full SSA DMF.
- Agencies lack accurate and timely information about individuals' earnings and overall income.

7.1 Program Design

Some statutes mandate aspects of the design of programs that create complications for Payment Integrity. This frequently occurs by the introduction of risky or complex eligibility criteria.

Risky criteria are found, in particular, in programs in which eligibility is heavily dependent on timely beneficiary self-reporting of "life changes." In the SSI program, for example, benefits for the upcoming month must be paid on the first of the month. However, if the beneficiary's income has increased to the point where they are no longer eligible for the program but they do not report this to SSA, then they will continue to receive benefits. It may take several months for SSA to receive income information from other sources that alert it to the beneficiary's change in eligibility, but by then perhaps thousands of dollars of improper payments have already been made.

The EITC may be the worst case of complex eligibility criteria in a federal means-tested program. It required 17 pages in the 2014 Form 1040 instruction book to guide taxpayers and tax return preparers through the eligibility criteria and calculations (including tables) for the credit. The next closest, the Child Tax Credit, took two pages of explanation, while most credits required less than ¼ of a page. The statutory complexity of the EITC is very confusing for taxpayers and tax return preparers and increases the chances of filing errors.

Other program design choices that can create challenges include:

- Whether a program will be administered by the federal government or the states. Many states choose to administer programs in different ways, some more effectively than others, based on priorities, capabilities, or funding. Two well-known examples of this are Medicaid and SNAP. Federal agencies often have difficulty overseeing the numerous approaches, definitions of terms, etc., among the states.
- Some legislation that requires agencies to give "notice" at the start of an application process in order to be able to stop a payment later. If this notice does not occur, then a payment cannot be stopped even if it is determined to be improper.

7.2 Definitional Issues

As previously mentioned, varying definitions of terms can create problems. Separate statutes often define the same terms in different ways, creating confusion for applicants and challenges for agencies in administering the programs. The term "household," for example, is defined differently for public housing, SNAP, and tax purposes, among others, and prevents the creation of a "single authoritative source" of relevant verification data for use across government.

- HUD's State Community Block Grant Program's working definition of household is "all persons occupying the same housing unit, regardless of their relationship to each other."
- USDA's SNAP defines household as "[e]veryone who lives together and purchases and prepares meals together…," with some exceptions.
- The filing status "head of household," for federal tax purposes, is someone who:
  - Is unmarried or "considered unmarried" on the last day of the year; and
  - Paid more than half the cost of keeping up a home for the year; and
  - Had a qualifying person living with them in the home for more than half the year (with some exceptions).

7.3 Prohibitions

The key statute that constrains federal agencies' ability to efficiently and effectively address Payment Integrity problems is the Computer Matching and Privacy Protection Act (CMA) of 1988 (P.L. 100-53). Although the CMA is notable in that it institutionalized the sharing of data sets among different federal agencies, it does place restrictions on the computerized matching of data sets within an agency or between agencies. Matching of data sets that would identify individuals who may be ineligible for a program, for example, is restricted to those data sets for which the matching had been publicly announced before the data was gathered, unless subsequent approval has been granted. Such matching is allowed if it only produces aggregated results, i.e., the total number of individuals who may not be eligible, but it cannot generate the names of those individuals without advance announcement or subsequent approval.[50] This subsequent approval involves a process that can take many months, and when completed the approval is only for a limited period of time. As a result, when agencies produce new data sets or learn of previously existing ones that might help them verify the eligibility of program participants or the validity of claims for benefits, they cannot simply begin matching those data sets to help prevent improper payments without first adhering to the detailed procedural requirements mandated by the CMA.

In addition to the CMA's clear mandates, some agency officials indicated that individuals in their organizations, particularly their Counsel component, adopt overly strict interpretations of the CMA. This excessive caution, in their view, hinders data sharing and matching beyond the literal statutory restrictions.

Proposals have been made in recent years to scale back the CMA restrictions or speed up the approval process. These include a McKinsey & Company recommendation to develop a

[50] Other notable exceptions include "matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons."

computer matching agreement "SWAT" team to accelerate the development and approval of inter-agency agreements, suggestions by agency officials to use anonymization to perform CMA-compliant analytics, and proposals by the Inspector General community to exempt them from the restrictions. However, the journey to approval for such matching remains long and cumbersome, and while it is unfolding, many improper payments that could be prevented may, instead, be issued.

The other major restriction that affects agencies in addressing Payment Integrity is that placed upon IRS' ability to share income data with other agencies by Internal Revenue Code §6103. A number of major federal programs include income as a criterion of eligibility, but they must rely on sources other than IRS for income information to help make this determination. These sources, in many cases, are not as accurate, complete or timely as the data in IRS records.

7.4 Conclusions

- For some programs, legislative mandates or prohibitions create or exacerbate the potential for improper payments.
- The resulting inherent risk level in some programs means that those agencies may only be able to go so far in reducing certain types of improper payments.

7.5 Recommendation

13. Address statutes that appear to create or contribute to – via program design, definitions, etc. – improper payments in selected major programs;[51] efforts should include:
    - Analyzing relevant statutes to identify the specific language that appears to create or contribute to improper payments
    - Assessing the impact on Payment Integrity
    - Evaluating alternatives to the program design, definitions, etc.
    - Identifying other statutes, as well as federal regulations and policies, that contain similar wording that could also impact Payment Integrity
    - Proposing legislative, regulatory, and policy changes, as appropriate

[51] Aspects of this recommendation are also reflected in a recommendation MITRE made in December 2007 regarding eligibility determination for some means-tested benefits programs: address legislation impeding state progress, including strengthening partnerships with states to understand / resolve issues resulting from federal legislation.

8 Cultural Barriers and Obstacles Hinder Payment Integrity

Organizational culture plays a crucial role in shaping behavior in organizations, which directly impacts performance. However, there are different views on what it actually is and how it influences behavior.

One view is that organizational culture consists of the values and behaviors that contribute to the environment of an organization. This includes an organization's expectations that hold it together, as expressed in, among other things, its inner workings. As previously discussed, many agency officials described their dilemma in key programs between making benefits payments at a certain time, and making sure the payments were proper. Invariably they chose the former over the latter. The choice could be characterized as "mission over management" – choosing to make the benefits payments over ensuring proper stewardship of the funds. In some cases internally imposed constraints (e.g., interpretations of legislation and OMB guidance, internal agency regulations and procedures) dictate these choices. Clarifying government-wide expectations regarding Payment Integrity may help ensure that agencies more closely balance mission and management; for example, as previously discussed, the July 2015 GAO fraud framework emphasizes the importance of establishing an organizational culture to combat fraud at all levels of the agency, stating that an anti-fraud tone ("management") needs to be set that permeates the organizational culture.[52]

Culture is powerfully shaped by incentives; in fact, the best predictor of what people will do is what they are incentivized to do. Other than avoiding the scrutiny that comes with being on OMB's "high priority" list, most agencies did not seem to have strong incentives to resolve Payment Integrity challenges internally, or to assist other agencies with their challenges. For example, some agency officials indicated that programs within their agency were not motivated to share data. Some officials also expressed reluctance to share data with other agencies that could help them address their Payment Integrity challenges, professing an "it's ***my*** data" view with few or no incentives to share it externally. In fact, in some cases when agencies did share their data, the receiving agencies complained that it was not in an optimal format, the data definitions differed from theirs, the data was not as current as they needed, etc.

Organizational culture can be expressed in an organization's self-image, and how officials view their agency drives behavior. The study often found that even when there are very common issues across programs (between and even within agencies), such as applicant identity, agencies tend to approach their Payment Integrity challenges as if they are occurring uniquely in their own programs. This contributes to the existence of disjointed, disconnected technology systems ("silos") inside agencies, as well as across agencies, that were developed to meet the "unique" needs of a specific program; these disconnects can reduce their effectiveness and impact. The "unique culture" mindset often manifests itself, as well, in state-administered programs, where state-by-state approaches may vary significantly and the ability for the federal government to mandate, or even influence, change can be limited.

An emphasis on uniqueness perpetuates a "silo" mentality that can inhibit the identification of common challenges and solutions. Conversely, a view that incorporates domain-wide and government-wide approaches, that recognizes ecosystems and "systems of systems" (i.e., the trend away from stand-alone component systems to richly interconnected and increasingly

[52] A Framework for Managing Fraud Risks in Federal Programs (GAO-15-593SP, July 28, 2015)

interdependent systems that cross traditional boundaries), and that acknowledges that multiple agencies and levels of government are often involved in striving towards the same goals and outcomes, would better enable government to combat improper payments.

Finally, some officials believed that approaches to implementing the various improper payments mandates can hinder solutions. Agency and accountability officials indicated, for example, that the mandated estimating of levels of improper payments has value. However, they maintained that the resources spent doing this, as well as conducting (OIGs) the mandated annual IPERA compliance audits and responding (agencies) to those audits, might better be spent building and implementing solutions. Further, OMB Circular A-123, Appendix C guidance to OIGs provides for flexibility in their approach to the mandated annual compliance audits. As a result, some OIGs take a more comprehensive approach than others, which offers more value than strictly addressing compliance with the six IPERA reporting factors.

- Representatives from one OIG indicated they do not view doing the IPERA-mandated compliance review as a singular, isolated responsibility, but rather as part of their ongoing, overall assessment of their agency's improper payments situation; they have a broader vision than "just" compliance with IPERA reporting. This OIG relies heavily on rolling up results from the other audits performed during the year; very little additional field work is required for their overall assessment.
- Another OIG's representatives said they look at their agency's root causes and corrective actions at a high level in the IPERA compliance audit. The audit focuses on whether the corrective actions are actually reducing the improper payments. The OIG often points out to their agency that the corrective actions are not as effective as needed, so others should be tried. In their other, more in-depth audits during the year they look in detail at root causes and the effectiveness of agency corrective actions in specific program areas related to the reported improper payments.

8.1 Conclusions

- Agencies do not always link a focus on mission with a focus on stewardship of / accountability for funds.
- The current reporting and presentation of Payment Integrity results does not appear to sufficiently motivate significant improvement and may undermine agencies' ability to justify additional investments.
- Absent targeted incentives, a "silo" mentality will likely continue to hinder intra- and inter-agency sharing to address Payment Integrity challenges.
- Agencies and the audit community could work together more comprehensively to reduce improper payments.

8.2 Recommendation

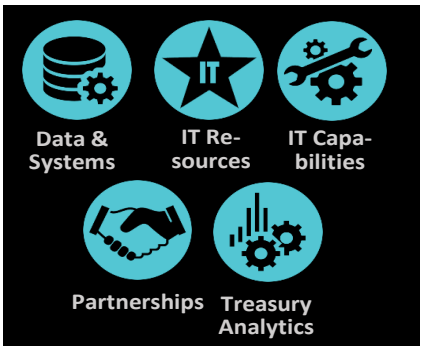
Some of the preceding recommendations contain elements that will positively impact cultural barriers and obstacles – providing incentives, helping reduce "silo" approaches, etc. These include:

- Assess the potential for a Cross-Agency Priority Goal for Payment Integrity and a government-wide Payment Integrity Roundtable (part of Recommendation 1)

- Assess existing metrics around corrective actions (Recommendation 4)
- Establish cross-agency / domain-wide work groups to share best practices and performance information, and establish mechanisms and methodologies to address data access and sharing issues (parts of Recommendation 10)

14. Facilitate greater audit community impact on helping agencies reduce their improper payments. In particular, OIGs could add value by adopting a broader vision than "IPERA reporting compliance" by expanding the scope of their IPERA compliance audits, as some of them already do, to include reviewing the effectiveness of agencies' identification of true root causes and corrective actions.

9 Technology Barriers and Obstacles Need to Be Resolved



Technology offers a critical line of defense in the fight against improper payments. Payments from federal programs are processed electronically, and the systems must contain the necessary controls, such as edit checks, to help ensure Payment Integrity. With the increasing volume and velocity of data, capabilities for automated data analytics, both real-time during prepayment processing and post-payment data mining, must be strong. As previously discussed, the availability of data – the right kind, at the right time, of the right quality – is a crucial factor in enabling needed analytics.

In the last several years, legislation has created the potential for cross-government capabilities that, if fully and effectively implemented, could enhance Payment Integrity. IPERIA mandated the DNP Initiative in 2012 to help ensure payments are proper. In 2014 the DATA Act authorized the establishment of a data analysis center in Treasury to help combat improper payments.

On the other hand, as previously discussed, technology can also be an enabler of financial crimes, in particular fraud. For example, the volume of tax filing fraud has increased in recent years as electronic filing (e-filing) of individual tax returns has grown. First, technology provides fraudsters the ability to purchase thousands of SSNs hacked from databases and bought and sold on the Internet. Second, they are then able, in just minutes, to fill out multiple tax returns using software programs and e-file them. While a proportional amount of fraud is found on paper returns, the sheer numbers that can be filed quickly through e-filing makes it a far more profitable venture. In fact, the relationship between technology and fraud has become so noticeable that the Institute for Fraud Prevention is sponsoring research at Northern Illinois University, Chatham University, and Slippery Rock University into the impact of a country's digital infrastructure on fraud levels and controls.

9.1 Data Standards and Systems Interoperability

An historic lack of data standards across government agencies, particularly financial data, has been a barrier to transparency, accountability, and data-driven decision making. While implementation of the DATA Act has driven some progress in this area (e.g., the May 9, 2015, publication of data standards for 57 data elements), a more comprehensive data standardization strategy could help reduce improper payments. For example, creating unique identifiers for awards and recipients, and linking awards to recipients, could assist Treasury's DNP solution in preventing duplicate payments, overpayments, and payments to the wrong recipients. Further data standardization actions could foster innovation and the use of data as an asset, and facilitate data sharing that could, in particular, help reduce improper payments.

A complicated and complex landscape of financial management computing systems exists across government agencies. Agencies rely on a diverse set of legacy financial systems such as SAP, Oracle, CGI Momentum, and "home-grown" systems that use different computing environments and are not interoperable with each other. This lack of systems interoperability makes the use of

a data centric versus a systems centric strategy important. Further, a standard data exchange format would help agencies publish and share their data on USASpending.gov and similar government-wide collection sites and move from agency silos to more strategic data-driven decision making that can help reduce improper payments.

9.2 IT Resources

A frequent obstacle for the federal government, as well as the states, is the sufficiency of resources for IT. In the case of Payment Integrity, this would include agencies' IT funding challenges that keep them from implementing robust IT solutions to prevent improper payments, such as developing needed edit checks in processing systems or performing real-time data analytics. Some agency IT departments are essentially shared services inside the agency, and the agency's Payment Integrity program has to compete for funding for analytic tools and data sets with other agency components. Many states, in particular, need to modernize their technology to enable such things as employer reporting of wages, which can be critical in preventing UI improper payments (see Appendix E for a case study of UI). In fact, a 2013 SAS / UBM Tech survey showed that only 43 percent of federal agencies and 29 percent of state / local agencies were using technology for fraud prevention. Half of the survey respondents indicated that cost was a barrier to adopting or planning to adopt anti-fraud technology, and that it was considered the most challenging aspect of deploying or using this type of technology.

As previously mentioned, human capital issues, especially the types of skillsets on hand in an organization, are often bigger obstacles to fighting fraud than technology challenges. The same SAS / UBM Tech survey found that a barrier to adopting technology to help fight improper payments was, in fact, staff technology skillsets – in particular, simply not knowing enough about anti-fraud technology. This repeatedly came up during the survey.

- Roughly one-quarter of respondents (27 percent of federal and 24 percent of state / local respondents) said they did not know enough about fraud prevention, in general, to make an informed decision regarding the use of technology.
- About one-third (33 percent of federal and 35 percent of state / local respondents) said they did not know enough about advanced analytics and business rules to make an informed decision.
- Roughly one-third (30 percent of federal and 34 percent of state / local respondents) said the same about continuous monitoring technology.

9.3 IT Capabilities

Some IT departments might feel challenged by their agency's needs for technology to help ensure Payment Integrity, such as analytics tools. Use of this type of technology might often not be in their "sweet spot," so the risk of failure could induce caution in procuring anti-fraud commercial tools and data sets. However, the role of technology is an important one that cannot be ignored. In fact, one financial crimes expert interviewed raised the question: What is the responsibility of CIOs to ensure their organizations are prepared to prevent, detect, and mitigate financial crimes of all kinds, including fraud? This expert suggested there may be a new future role for the CIO – to ensure technology is in place to prevent and detect improper payments.

9.4 Public-Private Partnerships

Ecosystems surrounding government services – or for that matter, domains such as healthcare – are increasingly interconnected and involve multiple stakeholders with similar, and sometimes competing, interests. The ability of any one organization or agency to accomplish meaningful change in these complex systems is limited by time, talent, and technology, among other factors. A potential solution exists in Public-Private Partnerships (PPP). PPPs provide a way for government, commercial, academic, and non-profit entities to collaborate on issues of mutual interest and to realize benefits that no single entity could feasibly achieve alone. A key characteristic of successful PPPs is accomplishing a shared mission and delivering value to the partners while sharing the burden of time, labor, and investment. By connecting talent, technology, and techniques across multiple stakeholders, the resulting pooled capability in the PPP enables significant impact at relatively low cost to any given partner.

9.5 Do Not Pay and DATA Act Implementation

Over the last several years, the Treasury DNP solution has endeavored to provide agencies with access to key federal databases for the purpose of identifying payments that may not be valid, such as a payment scheduled to be made to a deceased individual. The DNP solution has been promoted as a way to help solve Payment Integrity problems by emphasizing the use of key data and the breakdown of data silos. While the focus of the DNP solution to date has been on stopping improper payments before they are issued, Treasury officials indicated that their future vision includes targeted assistance for individual agencies, such as performing custom analytics, helping build risk models, and mapping processes to identify problem areas, in order to help identify potential improper payments earlier in processing so as to reduce the risk that they will be made. Treasury is working to leverage the expertise developed by the RATB's ROC in this endeavor.

While the current and future visions for the DNP solution are hopeful, progress and results to date have been mixed, and some accountability officials questioned whether agencies were using the DNP solution effectively. FY 2014 AFRs for numerous agencies showed extremely high false positive rates, in many cases reporting that all matches were false positives and no payments had been stopped. Some agencies reported very few "hits;" in one extreme case, an agency indicated that it had "only received one match, out of the more than eight million payments reviewed, in which the payment was stopped. The [agency] reviewed the single match and deemed that the payment was not improper." Treasury officials advised that they have examined the root causes of these results and indicated that by adding more identity information during FY 2015 they have dramatically reduced the false positives.

Finally, Treasury has begun implementing key aspects of the DATA Act that should help with government-wide Payment Integrity, in particular the statute's mandate for the development of certain data standards across the federal government, as previously mentioned. Another provision of the Act, §6(c)(1), authorizes Treasury to establish a data analysis center or expand an existing service to provide data, analytic tools, and data management techniques to support the prevention and reduction of improper payments by federal agencies. Treasury officials evaluated the provision, concluded that a Bureau of the Fiscal Service post-payment center in

Philadelphia[53] fulfills the intent of §6(c)(1), and decided not to invoke the authority the section provides.

9.6 Conclusions

- Data standards and interoperability issues reduce agencies' ability to efficiently address some improper payments.
- IT resources issues present significant challenges at the agency level.
- The vision for the Do Not Pay solution has not yet been fully realized.
- Full, effective implementation of the DATA Act could help resolve some of the issues.

9.7 Recommendation

15. Explore Public-Private Partnerships to cost-effectively bring to bear needed IT resources, data sets and skillsets otherwise unavailable.

[53] The Philadelphia Financial Center provides exception processing services to over 300 federal agencies, the primary ones of which are SSA, the Railroad Retirement Board, DOL, VA and IRS.

Appendix A Study Purpose and Methodology

Leadership of The MITRE Corporation, a not-for-profit organization that operates FFRDCs on behalf of federal government sponsors, recognizes the impact that the overall federal Payment Integrity situation has on government effectiveness and public confidence. Given the public interest nature of this challenge, MITRE conducted this independent, internally funded study to assess the underlying systemic factors that enable fraud and other improper payments and to explore government-wide solutions to improve Payment Integrity.

We acknowledge the considerable efforts already in place at OMB and across federal agencies focused on identifying, reporting and mitigating improper payments. Consequently, revisiting the existence and scope of the problem was not our focus. Instead, taking the current state as a "given," the objective of this study is to provide useful input and new insights to those efforts by addressing these key questions:

- What trends may be coming that could adversely impact the rate or the total dollars of improper payments?
- What are the root causes of the current improper payments?
- What obstacles must be addressed to make greater progress towards solutions?
- How can the federal government attack the problem in more effective, proactive ways?

To identify coming trends, we interviewed Payment Integrity experts in various private sector organizations and researched published reports from CBO, CRS, GAO, McKinsey & Company, et al. To understand the root causes of improper payments and obstacles hindering the government's ability to address them, we interviewed numerous federal agency, OMB, and accountability officials, and analyzed the FY 2013 and FY 2014 AFRs of 16 agencies. Finally, to identify more effective, proactive ways to attack the improper payments problem, we interviewed experts and researched published reports and documents to learn of private sector best practices; used information from the interviews with agency and accountability officials and the AFRs to pinpoint government best practices and successes; interviewed academic researchers and representatives of professional and non-profit organizations and a foreign government, all of whom were represented as having Payment Integrity expertise; and catalogued relevant MITRE research. We also gathered information and ideas pertaining to obstacles and solutions from a Senate Committee on Homeland Security and Governmental Affairs Hearing on the DATA Act, MITRE's Industry Day, and GAO's Data Sharing Community of Practice conference, all held during the time of the study. Table A-1 presents a complete listing of interviews, while documents reviewed are shown after the table.

Table A-1. Study Interviews

Agencies	
DOD (part of a group interview)	Department of Education (part of a group interview)
HHS – CMS (2 interviews)	HHS Office of the Assistant Secretary for Financial Resources
DHS (part of a group interview)	HUD (part of a group interview)

Agencies	
DOL	Department of Transportation (part of a group interview)
Treasury DATA Act Implementation Team	Treasury DNP Business Center
VA (part of a group interview)	IRS
National Science Foundation (part of a group interview)	OPM (part of a group interview)
Small Business Administration (part of a group interview)	SSA
Oversight and Accountability Organizations	
OMB Office of Federal Financial Management	OMB Resource Management Offices for DOL, CMS, IRS, and SSA
GAO (4 interviews)	Education OIG
HHS OIG	DHS OIG
DOL OIG (2 interviews)	Treasury IG for Tax Administration
SSA OIG (2 interviews)	Federal Bureau of Investigation – Criminal Investigation Division
Industry	
Anthem (Blue Cross of California)	Blue Cross Association
FICO	Thomson-Reuters
Academics	
North Carolina State University	University of Central Florida
Professional Organizations	
Founder, Association of Certified Anti-Money Laundering Specialists and Association of Certified Financial Crime Specialists, and former Assistant U.S. Attorney	Association of Certified Financial Crime Specialists
Association of Certified Fraud Examiners	Association of Government Accountants
Institute for Fraud Prevention	
Non-profit Organizations	
Partnership for Public Service	Sunlight Foundation
Foreign Government	
Australian National Audit Office	

We researched relevant statutes, Executive Orders, presidential memoranda, and OMB guidance (shown in Table 1-2) for federal requirements; the FY 2016 Program Integrity Funding Proposals for important funding requests; prior MITRE work products on improper payments and relevant internal MITRE research; and numerous internet websites for key information, such as irs.gov for information on the ACA premium tax credit and EITC, treasury.gov for information on the federal deficit and national debt, and finra.complinet.com for information on KYC program

requirements. We also researched the following documents to assemble a wide array of key information for use in the analyses.

- FY 2013 and FY 2014 AFRs for the following agencies.
  - Department of Agriculture
  - Department of Defense
  - Department of Education
  - Department of Health and Human Services
  - Department of Homeland Security
  - Department of Housing and Urban Development
  - Department of Labor
  - Department of Transportation
  - Department of Treasury
  - Department of Veterans Affairs
  - Agency for International Development
  - Environmental Protection Agency
  - General Services Administration
  - Office of Personnel Management
  - Small Business Administration
  - Social Security Administration
- CBO reports
  - "An Update to the Budget and Economic Outlook: 2014 to 2024." Pub. No. 5005, August 27, 2014.
  - "Growth in Means-Tested Programs and Tax Credits for Low-Income Households." Pub. No. 4505, February 11, 2013.
  - "Rising Demand for Long-Term Services and Supports for Elderly People." Pub. No. 4240, June 26, 2013.
  - "The 2013 Long-Term Projections for Social Security: Additional Information." Pub. No. 4796, December 17, 2013.
  - "The 2014 Long-Term Budget Outlook." Pub. No. 4933, July 15, 2014.
  - "The Pell Grant Program: Recent Growth and Policy Options." Pub. No. 4451, September 5, 2013.
  - "The Slow Recovery of the Labor Market." Pub. No. 4837, February 4, 2014.
- CRS reports
  - "An Analysis of the Distribution of Wealth Across Households, 1989-2010." RL33433, July 17, 2012.
  - "Military Base Closures: Socioeconomic Impacts." RS22147, February 7, 2012.

- "Noncitizen Eligibility for Federal Public Assistance: Policy Overview and Trends." RL33809, September 27, 2012.
- "Returning to Full Employment: What Do the Indicators Tell Us?" R43476, April 15, 2014.
- "Social Security Reform: Current Issues and Legislation." RL33544, January 15, 2014.
- "The Federal Budget: Overview and Issues for FY2015 and Beyond." R43472, April 11, 2014.
- "Treatment of Noncitizens Under the Affordable Care Act." R43561, May 21, 2014.
- "Unaccompanied Alien Children: Potential Factors Contributing to Recent Immigration." R43628, July 3, 2014.
- "Veterans' Benefits: Benefits Available for Disabled Veterans." RL34626, January 23, 2012.

- Census reports
  - "America's Families and Living Arrangements: 2012." P20-570, August 2013.
  - "An Aging Nation: The Older Population in the United States – Population Estimates and Projections." P25-1140, May 2014.
  - "BUSINESS DYNAMICS STATISTICS BRIEFING: Anemic Job Creation and Growth in the Aftermath of the Great Recession: Are Home Prices to Blame?" July 2013.
  - "BUSINESS DYNAMICS STATISTICS BRIEFING: Historically Large Decline in Job Creation from Startup and Existing Firms in the 2008–2009 Recession." March 2011.
  - "BUSINESS DYNAMICS STATISTICS BRIEFING: Where Have All the Young Firms Gone?" May 2012.
  - "Changes in Areas With Concentrated Poverty: 2000 to 2010." ACS-27, June 30, 2014.
  - "Dynamics of Economic Well-Being: Poverty, 2009–2011." P70-137, January 2014.
  - "Older Americans With a Disability: 2008−2012." ACS-29, December 2014.
  - "Poverty: 2000 to 2012." ACSBR/12-01, September 2013.
- 7 documents pertaining to the DNP Initiative, from sources such as OMB and the Bureau of the Fiscal Service
- GAO reports
  - A Framework for Managing Fraud Risks in Federal Programs (GAO-15-593SP, July 2015)
  - Anticipating and Meeting Accountability Challenges in 2014 and Beyond (GAO-14-591CG, May 20, 2014)

- FEDERAL EMERGENCY MANAGEMENT AGENCY Opportunities Exist to Strengthen Oversight of Administrative Costs for Major Disasters (GAO-15-65, December 2014)
- Financial Audit: U.S. Government's Fiscal Years 2013 and 2012 Consolidated Financial Statements (GAO-14-319R, February 27, 2014)
- Financial Audit: U.S. Government's Fiscal Years 2014 and 2013 Consolidated Financial Statements (GAO-15-341R, February 26, 2015)
- GOVERNMENT EFFICIENCY AND EFFECTIVENESS Opportunities to Reduce Fragmentation, Overlap, Duplication, and Improper Payments and Achieve Other Financial Benefits (GAO-15-440T, March 4, 2015)
- HIGH-RISK SERIES An Update (GAO-15-290, February 11, 2015)
- HURRICANE SANDY FEMA Has Improved Disaster Aid Verification but Could Act to Further Limit Improper Assistance (GAO-15-15, December 2014)
- IMPROPER PAYMENTS Government-Wide Estimates and Reduction Strategies (GAO-14-737T, July 9, 2014)
- Improper Payments: Inspector General Reporting of Agency Compliance under the Improper Payments Elimination and Recovery Act (GAO-15-87R, December 9, 2014)
- INDIVIDUAL DISASTER ASSISTANCE PROGRAMS Framework for Fraud Prevention, Detection, and Prosecution (GAO-06-954T, July 12, 2006)
- Standards for Internal Control in the Federal Government (GAO-14-704G, September 10, 2014)

- OIG reports
  - Fraud Risk Performance Audit of the Social Security Administration's Disability Programs (SSA OIG / Grant Thornton, A-15-15-25002, April 2015)
  - FY 2014 IPERA compliance audit reports from the following OIGs:
    - Department of Commerce
    - Department of Defense
    - Department of Education
    - Department of Energy
    - Department of Health and Human Services
    - Department of Homeland Security
    - Department of Housing and Urban Development
    - Department of Labor
    - Department of Transportation
    - Department of Treasury
    - Department of Veterans Affairs
    - Office of Personnel Management

        - Small Business Administration
        - Social Security Administration
    - Overpayments in the Social Security Administration's Disability Programs – A 10-Year Study (SSA OIG, A-01-14-24114, June 2015)
    - The Internal Revenue Service Is Working Toward Compliance With Executive Order 13520 Reporting Requirements (TIGTA, 2015-40-009, December 29, 2014)
- Professional sources
    - *Association of Certified Financial Crime Specialists*. "CFCS Certification Examination Study Manual." 4th edition. 2014.
    - *Association of Certified Fraud Examiners*
        - "Fraud Examiners Manual." U.S. Edition. 2014.
        - "Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study." 2014.
        - "Technologies on the Horizon." *Fraud Magazine*. March – April 2015.
    - *Association of Government Accountants*. "Developing a Shared Vision for 21st Century Accountability." Executive Report. December 2014.
    - Bone, Kristin, Pasquale Nigro and Kirk Petrie. "Caught in the Middle: How Government Contractors – and Other Businesses – Can Use Analytics and Continuous Monitoring to Address Improper Payment Risk Across the Value Chain." *Deloitte Review*. 2011.
    - *Committee of Sponsoring Organizations of the Treadway Commission*. "Internal Control – Integrated Framework." Executive Summary. May 2013.
    - *Gartner*. "Top 10 Strategic Predictions for 2015 and Beyond: Digital Business Is Driving 'Big Change'." October 4, 2014.
    - *GovWinIQ from DelTek*. "Technology Strategies for Federal Waste, Fraud, and Abuse – Federal Special Report." February 2013.
    - *IDC Health Insights*
        - "Best Practices: U.S. Healthcare Payer Fraud, Waste, and Abuse Services." January 2015.
        - "Best Practices: U.S. Healthcare Payer Fraud, Waste, and Abuse Solutions." May 2014.
        - "Business Strategy: U.S. Healthcare Payer Fraud, Waste, and Abuse Solutions Marketplace Overview." May 2014.
        - "IDC MarketScape: U.S. Healthcare Payer Fraud, Waste, and Abuse Solutions 2014 Vendor Analysis." April 2014.
    - *Journal of Government Financial Management*. Summer 2014.
        - Dixon, Calandra and Wendy Morton-Huddleston. "Key Practices to Sustain and Renew Your Commitment to Ending Improper Payments."

        - Kalustyan, Ray. “Taking a Proactive Approach to Improper Payments.”
        - Steinhoff, Jeffrey and Danny Werfel. “Are You Combat Ready to Win the War Against Improper Payments?”
        - Williams, McCoy. “Challenges Remain in Agencies' Efforts to Identify and Reduce Improper Payments.”
    - *KPMG Government Institute*. “A Practical Look at How Government Agencies Can Reduce Improper Payments.” 2011.
    - Lipman, Paul. “Keeping up with Criminals: Reducing Cyber Security Cost and Complexity.” *Enterprise CIO Forum*. May 21, 2015.
    - *McKinsey Global Institute*. “Disruptive technologies: Advances that will transform life, business, and the global economy.” May 2013.
    - “President's Management Advisory Board Approved Recommendations.” September 7, 2012.
    - *SAS*. “The State of Fraud in Government: Agencies Armed Against Fraud.” 2013.
- Academic sources
    - Clemmons, Anna. “Predicting Crime, 140 Characters at a Time.” *University of Virginia Alumni News*. Winter 2014.
    - Marquardt, Michael and David Schwandt. “Organizational Learning: From World-Class Theories to Global Best Practices.” 1997.
    - Spradlin, Dwayne. “Are You Solving the Right Problem?” Harvard Business Review. September 2012.
- News media sources
    - “Even the Tax Man Has a Taxing Time.” *The Wall Street Journal*. April 15, 2015.
    - *Government Designed for New Times*
        - “A Closer Look at Open Data: Opportunities for Impact. Undated.
        - “How Government Can Promote Open Data and Help Unleash Over $3 Trillion in Economic Value.” Undated.
- “As Mobile Commerce Grows, M-Commerce Fraud Grows Even Faster.” *Payments.com*. 2015.

The study research, especially the formulation of potential solutions and recommendations, was guided by the set of principles shown in Table A-2. MITRE presented these principles to and sought input from OMB, the Chief Financial Officers Council, and the Council of the Inspectors General for Integrity and Efficiency.

Table A-2. Study Guiding Principles

Title	Description
Focus on Prevention and Deterrence	Preventing / deterring fraud and other improper payments is preferred to detecting them after processing, and especially to making the payments and then attempting to recover them ("pay & chase").

Title	Description
Emphasis on Government-wide and Domain-wide Solutions	Solutions to address cross-government (e.g., identity, eligibility) and cross-domain (e.g., disaster response and recovery, food and nutrition) challenges will be emphasized.
Emphasis on Solutions, Not Estimation	Emphasis will be placed on finding solutions to help resolve significant improper payments problems, vs. estimating the degree of the problems.
Collaboration on Common Challenges	To the extent that is practical, feasible, and cost-effective, agencies will collaborate and share services and approaches for common challenges.
Broad Application of Solutions	Solutions with the broadest possible application will be preferred, in order to bring benefits to both federal programs that are being measured / reported and those that are not being measured / reported.
Enabling Flexible Guidance and Requirements	Policies addressing improper payments should remain fairly constant over time, but guidance and requirements will be flexible to accommodate future technology changes or more information.
Focus on Data and Analytic Approaches	Requirements for addressing improper payments government-wide or across domains will focus on data (types, exchange, etc.) and analytic approaches over specific technology and tool requirements.
Changes to Statutes	Changes to federal statutes and Executive Branch directives may be proposed if there is a compelling reason.
Changes to Policy, Guidance, and Requirements	Overlaps, conflicts, and inefficiencies in government-wide and agencies' policies, guidance, and requirements can be identified and proposed for change.
Availability of Funding	Limited funds to invest in system changes will be available based on agency need if the investment has a direct positive impact on reducing improper payments and if there is reasonable assurance that the reduction will be achieved.
Cost-Benefit Approach	While it may be theoretically possible to achieve a level of zero improper payments, doing so would likely cost significantly more than the benefits realized.
Existing Statutes' Mandates	Because agencies' program structures, actions authorized, etc., are often mandated by statute, absent changes these mandates must be adhered to.

The study reflects a qualitative analysis based on interviews, observations, literature and document research, and informed interpretation. Since MITRE's conclusions revolve primarily around how agencies address Payment Integrity, not the quantitative results that they report, the study does not cite extensive numbers – either in describing the present, or predicting the future.

Appendix B Case Study – Medicare and Medicaid

Healthcare represents a major segment of the U.S. economy, with 2016 expenditures projected to exceed $4 trillion. The Institute of Medicine has estimated that up to 10 percent of these expenditures are lost to fraud with another 20 percent or more lost to waste and abuse.

Medicare and Medicaid account for a significant portion of healthcare expenditures. The size and diversity of the programs make them particularly vulnerable to improper payments, including fraud. In fact, Medicare and Medicaid programs account for three of the top four individual programs with the highest FY 2014 improper payment dollar estimates:

- Medicare Fee-for-Service $46 billion 13 percent rate
- Medicaid $18 billion 7 percent rate
- Medicare Advantage (Part C) $12 billion 9 percent rate

These estimated improper payment amounts and rates do not necessarily fully account for healthcare fraud, which in FY 2014 could have involved an additional $96 billion for these two major CMS-administered programs.

The Medicare and Medicaid programs, and specifically their improper payments, are on the GAO 2015 High Risk List. On the positive side, the 2015 GAO report indicates that CMS has demonstrated strong commitment to reducing improper payments, particularly through its dedicated Center for Program Integrity. For example, CMS centralized the development and implementation of automated edits – prepayment controls used to deny Medicare claims that should not be paid – which will help ensure greater consistency in paying only those claims that align with national policies. Additionally, CMS awarded a contract to a Federal Bureau of Investigation-approved contractor that will enable the agency to conduct fingerprint-based criminal history checks of high-risk providers and suppliers. However, the GAO High Risk report also lays out further Medicare and Medicaid actions that need to be taken, stating:

- *To achieve and demonstrate reductions in the amount of Medicare improper payments, CMS should fully exercise its authority related to strengthening its provider and supplier enrollment provisions and address our open recommendations related to prepayment and post-payment claims review activities. Table 6 [pages 29 – 30 in the document] summarizes recommendations we made that are still open and procedures authorized by ACA that CMS should implement to help reduce Medicare improper payments.*
- *Medicare needs to improve use of automated edits; remove SSNs from Medicare cards to reduce identity theft risk; and implement actions authorized by [the ACA] …to combat fraud, waste and abuse.* [54]

Bottom line: Healthcare fraud is expected to continue to be significant in the coming years, and fraud scams are becoming more sophisticated, harder to spot, and more expensive to track. While providers continue to perpetrate fraud, increasing involvement by "consumers" – ranging from individuals to organized crime – is being seen. Evolving threats demand an adaptive, cost-effective defense, including innovative pilot studies to combat high-value healthcare fraud and a comprehensive program integrity strategy for managed care and other high risk improper payment areas. While CMS conducts such studies and has a strategy, GAO has observed that improvements are needed.

[54] HIGH-RISK SERIES An Update (GAO-15-290, February 11, 2015)

Appendix C Case Study – EITC

Between FY 2013 and FY 2014, EITC payments rose from $60 billion to $65 billion. The estimated improper payments also rose, from $14 billion to $18 billion, while the rate rose from 24 percent to 27 percent.[55]

IRS's processing of EITC claims on tax returns is generally good. Accountability officials indicated that they believed the tax return processing filters and controls are effective, and that the IRS does a good job of identifying suspicious EITC claims via its risk-based analytical approach.

Legislative issues appear to be the major cause of the difficulties in administering the EITC. Various statutes:

- Establish the eligibility criteria for receiving the EITC, which include a qualified relationship and the amount of time the child lived with the claimant during the year. However, data does not exist to verify these, and the eligibility criteria are very complicated. In fact, the IRS needed 17 pages in the 2014 Form 1040 instruction book just to explain eligibility criteria and calculations (including tables) for the credit.
- Require employers to provide Forms W-2 for employees, but not by January 31st each year when the IRS could use them to verify "current income" (one of the criteria for determining eligibility). Most tax returns claiming EITC are filed during January and early February. Treasury has proposed to Congress that the Form W-2 deadline be moved to January 31st to facilitate the use of earnings information in detecting EITC ineligibility.
- Require IRS to pay refunds within 45 days of the tax return filing due date. IRS can freeze the EITC portion of the refund, but if the claim proves to be valid then interest must be paid if the refund is issued past the 45-day period.
- Authorize IRS to automatically correct only a small number of issues on tax returns (known as "math error authority"). IRS can use math error authority to correct math or clerical errors or to adjust an EITC claim if a claimed child's SSN is not valid. However, the majority of potentially erroneous EITC claims do not contain these errors. If math error authority cannot be used, then IRS must initiate a formal examination of the tax return to address a potentially erroneous claim; the number of claims IRS can examine is limited by the availability of resources and the need to provide a balanced compliance program. Treasury has proposed that IRS be granted additional authority (referred to as "correctable error authority") to disallow a tax claim, including the EITC, when the claim is not supported by reliable government data sources, which could help IRS correct more errors and avoid burdensome examinations and taxpayer penalties.

IRS has also requested expanded authority to use the HHS National Directory of New Hires database for general tax administration purposes, including data matching and verification of taxpayer claims, which could help prevent the payment of improper EITC claims. Finally, recent years' declines in IRS budgets have meant fewer examinations overall, including examinations of EITC returns, which has led to more improper payments.

[55] According to the Treasury Department's FY 2014 AFR, IRS's estimates of EITC improper payments "…are primarily based on information from [a] reporting compliance study of individual income tax returns for tax year 2010 – the most recent year for which compliance information from a statistically valid, random sample of individual tax returns is available." These tax year 2010 returns were filed during calendar year 2011.

Bottom line: Absent legislative changes, IRS may very well be at the best level of EITC improper payments it can be right now, given what it is able to address. As GAO has reported, "Legislative action and significant changes in IRS compliance processes likely would be necessary to make any meaningful reduction in improper payments."[56]

[56] GOVERNMENT EFFICIENCY AND EFFECTIVENESS Opportunities to Reduce Fragmentation, Overlap, Duplication, and Improper Payments and Achieve Other Financial Benefits (GAO-15-440T, March 4, 2015)

Appendix D Case Study – Old-Age, Survivors, and Disability Insurance and SSI

In FY 2014, Old-Age, Survivors, and Disability Insurance (OASDI) payments were $863 billion with estimated improper payments of $5 billion, a rate of less than 1 percent, while SSI payments were $56 billion with estimated improper payments of $5 billion, a rate of 8 percent. The OASDI dollar amount increased from FY 2013, when it was $3 billion, while the SSI dollar amount decreased slightly from the previous year.

SSA gives senior leadership attention to improper payments and takes a number of actions to address them. However, two of its key actions are limited by available funding.

- SSI redeterminations – SSA planned to perform 2.6 million in FY 2015 but was only funded to do 2.3 million.
- Continuing Disability Reviews – SSA planned to perform 888,000 in FY 2015 but was only funded to do 790,000.

Both OASDI and SSI are challenged by legislative requirements around program design.

- These programs depend heavily on recipient self-reporting of changes that could affect benefits. This is challenging because recipients may not have sufficient incentive to share data that would change a payment and / or may not know or understand the requirements around self-reporting.
- Much of the data SSA needs to verify eligibility is time-critical. For example, in SSI both eligibility for payment and payment amounts are computed monthly, and payments are made for the upcoming month, i.e., payments made on May 1 are for the month ending May 31. Eligibility is based on lagging data required to be reported by mid-April, while the amount is based on data from the prior two months.

Bottom line: SSA understands that prevention is key, but is often driven into a “pay & chase” mode by legislative mandates.

Appendix E Case Study – UI

The UI program's workload dropped from FY 2013 to 2014, reducing UI payments significantly – from $67 billion to $48 billion. However, at the same time the improper payments rose to $6 billion and the rate to 12 percent. Based on DOL-published data for the most recent 12-month period ending March 2015, the fraud rate also rose from 2.9 percent to 4.1 percent.

DOL and state agencies have creatively tried to address the problems as they have defined them, but to date the efforts have been largely unsuccessful as measured by current and historic levels of improper payments. In fact, most of the structural impediments described below were actually created when the program was established under Titles III and IX of the Social Security Act of 1935 (P.L. 74–271) and in how they were subsequently implemented.

The current risk-based management approach, program structure and data issues are the primary impediments to making meaningful progress in reducing improper payments.

- The risk measures that are in place are primarily internally and administratively focused and are not based on the true root causes that need to be addressed. As a result, they do not communicate the real magnitude of the problems the program faces in order to either make material progress or justify more substantial efforts.
- States are in charge of how their programs are funded and administered; other than publishing arbitrarily defined performance standards, DOL has no effective measures or incentives to impact their efforts, raising questions about where the true accountability lies for the program results.
- It is unlikely that states can make cost-effective progress in addressing the significant challenges relating to an inability to adequately validate identity and verify eligibility due to the lack of timely, accurate and complete data needed.

Bottom line: Given current program requirements, including how legislatively imposed data sharing restrictions are interpreted and the lack of incentives to make any meaningful related changes, it is unlikely that the data necessary to address the true root causes will be available when needed. In addition, given that current measurements do not accurately reflect the real level of improper payments, in particular the level of fraud, it is unlikely that the evidence necessary to identify and support solutions that could make an impact will be considered or developed. Consequently, until these issues are addressed in a rigorous and systematic way this program will likely continue to cost taxpayers billions of dollars in improper payments.

Appendix F List of Abbreviations

ACA	Affordable Care and Patient Protection Act (P.L. 111-148)
AFR	Agency Financial Report
Census	Census Bureau
CBO	Congressional Budget Office
CFO	Chief Financial Officer
CIO	Chief Information Officer
CMA	Computer Matching and Privacy Protection Act of 1988 (P.L. 100-53)
CMS	Centers for Medicare & Medicaid Services
CRS	Congressional Research Service
DATA Act	Digital Accountability and Transparency Act of 2014 (P.L. 113-101)
DHS	Department of Homeland Security
DMF	Death Master File
DNP	Do Not Pay
DOD	Department of Defense
DOL	Department of Labor
EITC	Earned Income Tax Credit
ERM	Enterprise Risk Management
FAFSA	Free Application for Federal Student Aid
FEMA	Federal Emergency Management Agency
FFRDC	Federally Funded Research and Development Center
FFS	Fee-for-Service
FINRA	Financial Industry Regulatory Authority
FY	Fiscal Year
GAO	Government Accountability Office
GDP	Gross Domestic Product
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
IoT	Internet of Things
IPERA	Improper Payments Elimination and Recovery Act of 2010 (P.L. 111-204)

IPERIA	Improper Payments Elimination and Recovery Improvement Act of 2012 (P.L. 112-248)
IRS	Internal Revenue Service
ISAC	Information Sharing and Analysis Center
IT	Information Technology
KYC	Know Your Customer
MITRE	The MITRE Corporation
OASDI	Old-Age, Survivors, and Disability Insurance
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PARIS	Public Assistance Reporting Information System
PII	Personally Identifiable Information
PIRAC	Payment Integrity Research and Analysis Capability
PMO	Program Management Office
PPP	Public-Private Partnership
RATB	Recovery Accountability and Transparency Board
ROC	Recovery Operations Center
ROI	Return on Investment
SAR	Suspicious Activity Report
SSA	Social Security Administration
SNAP	Supplemental Nutrition Assistance Program
SSI	Supplemental Security Income
SSN	Social Security Number
TANF	Temporary Assistance to Needy Families
UI	Unemployment Insurance
USDA	United States Department of Agriculture
VA	Department of Veterans Affairs