



# FIVE WAYS TO FIGHT FRAUD, WASTE, AND ABUSE IN \$3 TRILLION CORONAVIRUS RELIEF AID

## Background: Historical Improper Payments Problems Confront the Government

The federal government annually makes trillions of dollars of payments of all kinds to private citizens, businesses, state and local governments and NGOs for Medicare benefits, disability claims, tax credits, grants, and loans to small businesses. The great majority of these are proper and provide benefits to the individual or business to support a need. However, since 2003, agencies estimate they have made about \$1.7 trillion in improper payments—payments that either should not have been made or were made in the wrong amount due to agency processing errors, applicant errors, or fraud. The estimate for fiscal year 2019 alone was approximately \$175 billion—an increase of \$24 billion over the previous year. These needless expenditures restrict spending options, add to the federal debt, enrich criminals, siphon off funds needed to serve the interests of the American public, and undermine public confidence in government. This critical issue has been the focus of three Administrations, multiple legislative actions, and the Government Accountability Office (GAO) in its high-risk series and reporting on fragmentation, overlap and duplication in government programs.

## Current Events Have Brought a Massive Response

The great majority of improper payments to date have occurred under the “normal business of government.” However, experience shows that when special circumstances require large outlays in government money to address significant events which threaten our nation, the need to make the payments fast and timely, while getting them to the right person or business to address their need, is critically important if the money is to achieve the intended result. While events such as the enactment of the American Reinvestment and Recovery Act of 2009 (ARRA) and Hurricanes Sandy and Katrina presented unique challenges to ensuring proper payment of benefits, the recent passage of the Coronavirus Aid, Relief, and Economic Security (CARES) Act presents an even greater imperative to get payments right. As of April 2020, the U.S. Congress and the Trump Administration have authorized nearly \$3 trillion in new money associated with four bills to counter the human and economic cost of the Coronavirus pandemic. This figure promises to increase even more with consideration of a potential fifth legislative proposal.

Since 2003, agencies estimate they have made about **\$1.7 trillion** in improper payments.

The estimate for fiscal year 2019 alone was approximately **\$175 billion**—an increase of **\$24 billion** over the previous year.

Like other disaster responses, the response and economic stimulus legislation recently passed contains benefits for individuals (e.g., direct payments, increased program benefits) and businesses (e.g., loans) paid out using a combination of new programs, one-time-only actions, and significant modifications to existing benefit programs. We believe that similar historical events offer important lessons learned for application today, especially the need to take measures to ensure the integrity of the payments and distribution of funds provided by the response and stimulus measures in order to achieve the outcomes and impacts intended.

## Valuable Lessons Can Be Learned from Past Events

In February 2016, The MITRE Corporation, a not-for-profit company that operates federally funded research and development centers on behalf of Federal sponsors, published a broad study of the problem space, “Government-wide Payment Integrity: New Approaches and Solutions Needed.” Using key lessons learned from numerous sources and our firsthand experiences – including the implementation of the ARRA, operation of the Healthcare Fraud Prevention Partnership (HFPP), and events such as Hurricanes Sandy and Katrina – MITRE recommended a more comprehensive and government-wide approach to address the problem. This included:

- Strengthening the focus on government- and domain-wide payment integrity issues by establishing a cross-government senior leadership group and a Cross-Agency Priority Goal
- Focusing on risk management and identifying true root causes of payment issues in order to create more effective corrective actions that would enhance the prevention of errors and deterrence of fraud vs. the detection of them after they have occurred (often called “pay & chase”)
- Creating collaborative structures to bring parties together to confront shared payment integrity challenges by:
  - Using public-private partnerships to jointly confront domain-wide problems ranging from common identity and eligibility verification issues to widely used fraud techniques
  - Establishing Information Sharing and Analysis Centers— ISACs—like those used to identify and fight cyber-crime or identity theft tax refund fraud
- Developing and sharing advanced analytics and mechanisms and methodologies to promote data access and sharing

The federal government has made strides in addressing the

payment integrity challenge. In 2018, for example, the President’s Management Agenda established a Cross-Agency Priority Goal, Getting Payments Right, with a cross-government Executive Steering Committee which has promoted government-wide efforts. But with the passage of the CARES Act and other measures in response to COVID-19, immediate action will be needed to establish the collaboration, data sharing and analytics across government and the private sector to prevent and detect payment errors and fraud that could undermine the credibility and effectiveness of these efforts.



## Coronavirus Relief and Stimulus Funding Presents Risks

The scope and scale of the response to the COVID-19 pandemic eclipses the 2009 ARRA and any federal stimulus before or after. The combination of the pandemic’s public health and personal impacts with the resulting economic impacts warrants fast and bold action. But we know from experience that unprecedented conditions such as these result in both preventable payment errors and opportunities for those who seek to take advantage of the situation for their own criminal means. Conventional wisdom says that 7% of government spending is subject to fraud, waste and abuse. This was an estimate often cited by Earl Devaney, the former chairman of the Recovery Accountability and Transparency Board (RATB) established to oversee the spending of stimulus money from the ARRA of 2009. This is an unacceptable percentage that when applied to nearly \$3 trillion in spending represents potentially \$210 billion paid out in error or to fraudsters. The chances of errors occurring are increased as claimants who are under duress and not familiar with federal programs must navigate benefits application processes to seek financial assistance, and as agencies deal with a surge of claims while wanting to both get payments into the hands of legitimate recipients as fast as possible and be good stewards

of the taxpayer's money. Indeed, many of the changes directed by the CARES Act impact eligibility rules, application requirements and other instructions to the public that in normal times are often difficult to understand or follow, creating a greater potential for mistakes to be made by the applicant or the responsible agency. Meanwhile, the availability of trillions of dollars is an attractor to fraudsters who will exploit new requirements and already stressed and vulnerable federal programs like unemployment, disability and others to redirect to themselves monies that should go to legitimate, struggling claimants. The imperative for the government is to have a dynamic, agile capability to detect potential fraud and waste, while releasing the money now to provide the assistance so desperately needed by individuals and businesses alike and to stimulate the recovery. Examples of where we see the risk include:

- Specific to healthcare, e.g., with the increased emphasis on telehealth – providers billing for fraudulently prescribed durable medical equipment, pharmaceuticals, and testing that is not medically necessary as well as billing for services not rendered at all.
- With a surge in claims for various kinds of benefits such as Unemployment Insurance and the Supplemental Nutrition Assistance Program, e.g., the use of stolen or synthetic identities to apply for benefits.
- With fraudulent applications for, or misuse of money related to, business loans and various grants.
- With claims for the new advanced tax credits for paid sick and paid family and medical leave; these types of credits have historically been targets for fraudsters, especially where the credit is paid in advance of the tax filing.

## Efforts Urgently Needed to Prevent and Detect Fraud, Waste, and Abuse

Based on our independent study into the systemic issues that lead to errors and leave programs vulnerable to fraud and our work with federal agencies, including the RATB, the new Pandemic Response Accountability Committee needs to adopt practices and supporting technology to perform three distinct but related oversight activities:

**Sensing** – monitoring activities and accepting public feedback on people and organizations that are engaged in suspicious activity. The RATB relied on public “whistleblowers” and “good government” groups to do this, but new capabilities exist to more rapidly and comprehensively identify fraud schemes and disinformation campaigns designed to defraud the government or steal from deserving recipients.

**Analyzing** – the core analytic activities needed to root out suspicious patterns of behavior, entity relationships, and other means to better understand where money actually goes compared to where it should go.

**Acting** – making referrals to agency Offices of Inspector General or the Department of Justice, as appropriate, and providing government-wide recommendations to improve accountability over stimulus funds.

The Committee, along with all of the agencies responsible for implementing provisions of the Act, will need to identify the key risks to payment integrity presented by the response and stimulus packages in accordance with Office of Management and Budget Circular A-123 and GAO's “A Framework for Managing Fraud Risks in Federal Programs.” Then, we recommend that the Committee, agencies, and others draw on the lessons from fraud and error risk mitigations that have been successfully applied in the past by taking the following 5 key actions.

1. Establish under the Pandemic Response Accountability Committee a data aggregation and analytic capability, to partner with academia and the private sector and coordinate with relevant agencies. This team should apply advanced analytic tools, techniques and datasets from the public and private sectors to provide programmatic guidance to inform spending. The team should monitor spending activities; identify potential errors and find their root causes so they can be systemically fixed; advise agencies on how to simplify eligibility and application rules to best serve the public, minimize errors, and deter fraud; and partner with law enforcement agencies to root out and minimize fraud.



2. Establish domain-specific public-private partnerships with supporting ISACs, such as the Identity Theft Tax Refund Fraud ISAC and public-private partnership, led by agencies responsible for significant amounts of new spending. Through these mechanisms both government agencies and private sector entities will find ways to share information on common risks, emerging fraud campaigns, and ways to counter them.
3. Explore ways to develop and share more broadly advanced analytics approaches and data for the greater good. Analytics that have been shown to be effective but are not widely used, such as social media analytics, need to be more widely considered. Data sharing is now easier via provisions in the recently enacted Payment Integrity Information Act of 2019.
4. Seek temporary relief from statutory restrictions on sharing and using some datasets across agencies in order both to support verification of eligibility and to help individuals accelerate confirmation and receipt of benefits. This will also help identify potential cross-program fraud.
5. Avoid “pay & chase” by focusing on preventing errors and deterring fraud, rather than identifying them after-the-fact. Pay & chase is a fundamentally flawed approach. It is expensive and ineffective: agencies typically get less than 50% back. Fraudsters take advantage of that, with both the intended recipients and taxpayers losing out.

## Benefits Now and for the Long Term

These actions can be taken quickly, and we know from experience that they work. The ultimate objective is to ensure that the intended impact of the stimulus funds be realized in terms of both the response to the health crisis and the mitigation of and recovery from the personal and economic hardships wrought by this pandemic. Through actions such as these, the government would be better positioned to identify the indicators, the locations, the conditions, and more, that lead to improper payments and to proactively address them to prevent these payments. While some agencies are engaged in extensive data analytics, more needs to be done to create the partnerships and capabilities necessary to use data effectively across government to deter fraud and prevent improper payments. Furthermore, while certainly critical for the current situation, these successful fraud and error mitigations should also be kept in place to help strengthen government-wide payment integrity for the long term.

For information about payment integrity expertise and capabilities, contact Gordon Milbourn, [gmlbourn@mitre.org](mailto:gmlbourn@mitre.org).



As the nation faces this monumental challenge, it's vitally important to take these immediate steps to minimize fraud, waste, and abuse while ensuring that all Americans receive their full and accurate benefits.

*MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government to tackle challenges to the safety, stability, and well-being of our nation.*

**MITRE** | SOLVING PROBLEMS FOR A SAFER WORLD