



Minimizing Fraud, Waste and Abuse: Implementation of Improper Payments Elimination and Recovery Act Reforms

WHITE PAPER

Prepared by:
Paul Raffensperger and Frank D. Banda, Principals

February 4, 2011

Introduction

Because of the size and scope of government operations and transfer payments, even a relatively low error rate compounds into a significant dollar loss. According to the Government Accountability Office (GAO), the federal government was responsible for approximately \$98 billion in improper payments in FY2009, of which \$55 billion was in the Medicare and Medicaid programs. This loss diverts much-needed resources from their intended use and erodes the confidence of the citizenry in its government's ability to operate large programs effectively.

The Obama Administration has taken several bold steps to significantly reduce improper payments made by the federal government. In response, the administration issued Executive Orders in November 2009 and March 2010 that increased transparency and agency accountability for identifying and recapturing improper payments. In June 2010, a Presidential Memorandum was issued that requires the establishment of a Federal Do Not Pay List (DNPL) and directed the Office of Management and Budget (OMB) to develop and submit a plan by October 18, 2010, to integrate DNPL databases in order to make them accessible to agencies through a single point of entry. It also required OMB to issue guidance by December 18, 2010, outlining the actions agencies must take to ensure that available databases are checked before payment and award to prevent improper payments. The guidance also identifies best practices and databases that should be used to ensure that only eligible recipients receive government benefits or payments.

To help inform the guidance being developed by OMB and the establishment of the DNPL, the Partnership Fund for Program Integrity and Innovation (The Partnership Fund) has requested input and recommendations based on relevant lessons learned and best practices. Based on our experience managing the proper distribution of billions of dollars of federal funds to recipients, we feel that the DNPL, though it provides a solid foundation, should actually serve as the basis for a more holistic quality assurance environment. In this paper, we outline what such an environment would integrate with the payment process, the components of the quality assurance environment, and best practices for its implementation.

Why Do Improper Payments Occur?

Any proposal for improving the government payment process must begin with awareness of the factors that increase the risk of improper payments. In our experience, we have found that the factors outlined below can be particularly problematic.

Urgency of delivery – In many situations driven by legislative mandates, political dynamics and public demand, urgency of need becomes the most obvious driver for payments to affected citizens. In the face of public outcry for financial assistance and support, an agency may rush to respond without sufficient analysis of the adequacy of personnel, processes and systems behind such payments, resulting in payments to ineligible individuals or entities.

System constraints – While agencies have systems to disburse, verify and track payments, many of these systems lack the scalability and flexibility to meet specific disbursement requirements or a sizable increase in transaction volume (such as that which occurs after a natural disaster). Where payment capabilities do exist, there may not be adequate resources to perform the modifications required. As a result of these deficiencies, payments may be made to individuals or entities that are ineligible, to an incorrect address, and in some cases, to deceased individuals.

Lack of adequate staffing and oversight – Budget cuts have left many payment offices short of staff. These internal resource constraints may result in staff taking shortcuts and quality control processes being circumvented. Proper oversight is necessary to ensure that processes are followed and controls are working as intended.

Lack of training – No matter how strong the payment process is, it will generate errors if manned by a poorly trained workforce. Individuals lacking the necessary formal education and proper training will invariably make mistakes that contribute to improper payments.

Poorly defined accountability among federal, state and local stakeholders – Without clearly established and mutually agreed-upon reporting and monitoring requirements, the responsible federal agency may not be able to determine in advance whether the state agency has the proper financial management systems in place to fulfill its accounting and reporting responsibilities.

A Schematic View of the Payment Process

To understand the improper payment challenge, it is helpful to break the overall payment process down into three distinct segments – pre-payment, payment and post-payment. In the pre-payment phase, the payor identifies the request for payment and determines if it is appropriate. In the payment phase, the payor schedules the payment and either makes it or, as with most federal agencies, passes the payment request to the U.S. Treasury for payment. In the post-payment phase, the payor updates internal accounting records to reflect settlement of the obligation and subjects the process to review and audit. Improper payment issues can arise in each of these three phases.

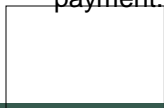
While the establishment of the DNPL provides a solid foundation in reducing waste, fraud and abuse, to have maximum impact it must be part of a larger quality assurance environment that interacts with the entire payment process at various critical points. This is particularly true given the fact that preventing pre-payment errors is significantly more effective than post-payment recovery of improper payments. At the same time, however, the checks afforded by the DNPL must be implemented so as to minimize the disruption of the flow of valid payments. By establishing and implementing a Federal Do Not Pay Quality Assurance Framework, agencies can achieve significant reductions in improper payments and high, sustainable rates of payment accuracy over the long term. Rigorous, proven quality assurance processes will ensure that, as agencies use the DNPL, they are not stopping valid payments based on flaws in business process or systems, or because of poor data quality.

At a high level, the payment process with an integrated quality assurance environment can be viewed as shown in the graphic below.

Error! Reference source not found.

Process highlights:

- Prepayment processes should continue to operate “as is” through the determination of eligibility for payment.



- DNPL search criteria should be established and validated using reliable third-party data sources to reduce the likelihood of “false-positives” and “false-negatives” that may result from comparing agency payment information to the DNPL databases. The validated information should be used to search the Federal DNPL system.
- An exception handling process must be established to address invalid search criteria.
- Once the DNPL search criteria are validated (as a final check before approving, certifying and scheduling the payment), the agency would access the Federal DNPL system to make a determination as to whether the payee is on the list of people or entities excluded from receiving federal payments.
- If the payee is listed in the DNPL as a party that should be excluded from payment, the payment request would be denied, not scheduled for payment, and forwarded to exception processing. A data flag would be sent in the financial management system to indicate that a problem exists and to put a hold on the payment until it is resolved through the exception processing. Policies will need to be created to address those payments that cannot be made because the entity is on the Federal DNPL.
- In exception processing, the government should research the payee and rationale for excluding the payee from payment and either confirm that the payee should be excluded or approve the payee for payment based on additional findings. The exception processing staff should document all decisions and rationale, as well as any contacts with the payee.
- Both payments that are validated during the original pass through the DNPL system and those that are validated during exception processing should be approved, certified and scheduled for payment using existing agency and Treasury processes.
- New initiatives should utilize a “pilot program” approach to prove the concept of operations.
- Independent quality control should be used to test and monitor the integrity of systems and processes, and to identify improvements to quality.
- Investing in proper training on the front end significantly reduces the number of discrepancies and increases productivity in the payment process.

The Four Pillars of Quality Assurance

At a more granular level, a successful DNPL quality assurance environment requires four specific elements: software controls, process controls and exception handling, payment processes and data integrity. This section explores each of those in turn.

Software Controls

The federal DNPL mandate will require changes not only to processes, but also to agency systems. Potential problems must be identified and mitigated through proper planning. Several best practices can be identified:

- Software and systems that govern payment processes must be tested continuously to ensure that the software is operating as intended and properly reflects the changes in eligibility requirements that often occur as programs mature. One method of monitoring software modifications is through software configuration management (“version control”). User Acceptance Testing (UAT) should be used in the testing process to ensure that there is a uniform process for accepting modifications.
- Documentation of hardware, systems and applications must be created (and updated regularly) as the systems are brought online. The documentation should include all software application and user access policies and procedures. In addition, security policies must be created and agreed upon by all administrators. Along with a security policy, new security assessments must be done whenever significant infrastructure changes are made.
- There should be regular audits of systems user access, as well as user roles, to provide assurance that the systems are working as intended and to identify problems that require resolution. These audits can be performed by an internal audit or an independent audit group.

Process Controls and Exception Handling

The DNPL quality assurance environment should contain policies, processes and systems for controlling and handling DNPL exceptions—any information or action that falls outside of a defined standard. These exceptions must be addressed in an efficient and effective manner and with the required level of diplomacy and due process. By following well-defined policies and processes, and using a workflow and management system covering these activities, exceptions will be consistently handled and properly closed according to an agency’s policies. An exceptions process should also be used to identify an error in the logic of the automated process or an inefficient automated process.

The process of resolving exceptions varies among business processes but in general includes manual review of existing information, clarification with a third party and clarification with the payment recipient. Exceptions indicate that a payee is not ready to be formally classified as eligible to receive a payment. Resolving an exception may uncover information that disqualifies a payee from receiving a payment. Exceptions can be generated automatically through a system import or manually to an exception queue. These exceptions must be tracked and aged in an exception management system until resolution.

We have developed the best practices described below for handling exceptions.

- The first step in exceptions processing is a manual review of the provided information to compare it with what has been determined as the acceptable standards. An automated message may prompt the user to an exception in the queue. The user reviews the data and determines whether the information is accurate and sufficient to meet the criteria. If the data are accurate and sufficient, the user updates the system of record to show that the criteria have been met, inserts comments documenting why and how the data are sufficient and clears the exception. Although the exception is completed, it is archived for future reference and audit support. If there does not appear to be a clear reason for the exception, the user can initiate an investigation into the logic of the exception.
- If there are erroneous or incomplete data, the user initiates the second step of the exceptions process, which is clarification with a third-party data provider. A request to clarify payee information is sent to the data provider for confirmation either through written correspondence or a secure data

exchange method. If the data provider is able to clarify the existing information and it is determined to be sufficient, the user updates the system of record and clears the exception.

- If the data provider is unable to clarify the data, the user initiates the last phase of the exceptions processing, clarification with the intended recipient. At this point, the user reviews the exceptions log to determine what information is creating the exception, or what information is missing, and outlines the deficiencies. The payee is sent a notification including a list of documentation that is required to resolve the issue and a request that it be sent back within a specific time frame. If the payee returns sufficient documentation, the user updates the system of record that the criterion has been met, documents why and how the data are sufficient and clears the exception. However, if the information provided is still considered deficient or the applicant is unresponsive, the system of record is updated to reflect that the payee is ineligible for payment, the comments are updated in the log and the exception is closed.

Payment Processes

Agency payment processes will need to be modified in order for the DNPL process to have maximum effect. Best practices are described below.

- All systems should produce an audit trail of systems users and payment processors. By having the audit logs, an agency can trace identified problems to specific users. This is necessary as part of the oversight and quality assurance process. A problem resolution process should be developed so as to improve the payment process.
- There should be clear and specific written guidelines that must be followed when approving and making a payment to a recipient. These guidelines must be tested when a new process is introduced to provide quality assurance over the process.
- A manual review is needed (at least on a test basis) to verify that the new DNPL payment processes are followed and the necessary support is complete before a payment can be made. Our experience in large-scale government projects has shown a substantial reduction in improper payments by implementing a final high-level of review before authorizing and approving payment.

Data Integrity

Ensuring the quality of data to be used in the DNPL--both payment request data normally initiated by the prospective payee and data from the DNPL source databases--is essential for reaching the correct decision regarding the processing of payment. There are inherent risks affecting the quality of both of these types of data. During the registration process, payees are required to provide individual or entity information. Often, however, that information is not verified for accuracy. A critical portion of federal DNPL process rectified that shortcoming by comparing payee data with five national databases.

How that comparison is made, however, can have a significant effect on the strength of the data assurance program. In one program we managed, for example, we found that it was better to match records by Social Security Number than by unique identification number, as the former has attached to it a wider and more accurate range of supporting information. We then compared the agency's data with the data provided by the applicant and supplemented or corrected the data where appropriate. This

method of data matching allowed for more accurate payment determinations and less risk of improper payments.

An Important Source of Public Trust

Significant amounts of federal funds are paid to individuals and organizations that are defrauding the government. Federal payor organizations, their employees and their support contractors need to have credibility with citizens, lawmakers and Administration leaders. These constituencies must have confidence that federal funds are being carefully managed by the organizations to which they have been appropriated, and that perpetrators of fraud will be identified and dealt with, and respective funds recovered.

To create such credibility, those responsible for administering programs and payment processes need to build a culture of accountability and ensure that those involved in program operations, quality assurance and oversight are free of conflicts of interest. Agency and program leadership must instill a culture of accountability by making quality assurance a priority, supporting its implementation and rewarding the achievement of successful outcomes. Throughout the implementation process, expectations and accountability must be clearly established and communicated. With the passage of the Improper Payment Improvement Act and the establishment of the federal DNPL, the Administration and Congress have taken an important first step in establishing the direction and tone. Department and agency-level officials must leverage this top-level attention and drive accountability down through their workforce, by ensuring that performance agreements and contracts include requisite goals, objectives and metrics related to improper payments.

Reznick Government

Independent accounting firms can play an important role in evaluating the quality of ongoing operations, establishing and implementing the verification process, and conducting regular reviews and audits. The experience of Reznick Government includes management, administration, monitoring and oversight of the distribution of nearly \$10 billion in federal funds for Gulf Coast disaster recovery programs, as well as more than 20 years managing Community Development Block Grant (CDBG) and Housing and Urban Development compliance programs. Specific relevant experience and past performance examples include those described below.

- Reznick Government was directly involved in the distribution of more than \$2.5 billion under the Mississippi Development Authority for CDBG disaster recovery programs following Hurricane Katrina, during which we were responsible for establishing stringent application, validation and approval processes to distribute funds, and for creating safeguards to prevent fraud, waste and abuse. We not only determined and validated eligibility, calculated benefits and managed delivery of the funds, but also developed technology designed to evaluate and process thousands of applications, simplifying the process and ensuring compliance with regulations and requirements.
- For the Texas Department of Housing and Community Affairs' Homeowners Assistance Program, Reznick Government was solely responsible for overseeing the benefit determination phase, which included creation of a system for determining the benefit calculation and how applicants would be notified, and for ensuring that claims for unpaid and outstanding insurance claims were subrogated

back to the programs. We also developed processes to manage the distribution of funds from approval to final draw and planned the use of administrative systems, software and infrastructure to manage the programs effectively.

- Reznick Government recently worked to assess, evaluate, document and test the Federal Housing Administration's (FHA's) internal control over financial reporting and developed a comprehensive and sustainable system to meet the requirements of FHA, the Federal Managers Financial Integrity Act, OMB Circular A-123 and the Federal Financial Management Improvement Act. We have established processes to identify control issues and quickly address them.

Successful payment processes require professional, disciplined project management expertise. Reznick Government has professionals certified by the internationally recognized Project Management Institute as Project Management Professionals. This globally recognized credential demonstrates our professionals' project management experience, knowledge, skills and capability to lead and direct project teams. Our project management services include:

- PMO implementation
- Full lifecycle program development and implementation
- Requirements assessment and planning
- Business process development
- Risk management
- Scheduling and cost control
- Fraud, waste and abuse control
- Project administration and oversight
- Compliance and monitoring
- Staff augmentation

To learn more about Reznick Government and our services for federal, state and local governments, visit www.reznickgovernment.com.

This publication contains only general information and is not intended by Reznick Group to be a rendering of accounting, business, financial, investment, legal, tax or any other professional advice or services. This publication is not a substitute for any professional advice or services.