IBM Counter Fraud and Improper Payments for Government

Detect, respond and reduce improper payments for Health and Human Services

Highlights

- Pro-actively identify and prevent fraudulent activity earlier, before improper payments occur
- Maintain a robust network of compliant healthcare providers
- Simplify administrative procedures and automate to increase productivity
- Quickly distinguish fraudsters from law-abiding citizens
- Improve the effectiveness and efficiency of caseworkers and investigators
- Detect suspicious behaviors either retrospectively or at the time a request is filed
- Maintain the organization's image
- Employ enterprise intelligence to continuously adjust operations and stay ahead of trends

Social Services organizations are on the front-line of government efforts to deliver better outcomes to citizens with limited resources. Since funding for social services represents the single largest component of government spending, (an estimated 22 percent of OECD is based on government health and social program spending)[1], there is increasing pressure to do more with less and be as efficient as possible. This means balancing equitable serve to citizens with minimal waste and error. The problem is that fraud, abuse and improper payments are on the rise. These fraudulent schemes are being driven by both opportunistic individuals and sophisticated criminal organizations who are early adopters of technology and employ a dynamic agile business model. It is therefore incumbent for a government agency to base their counter fraud operations on technology and processes that can both scale to handle the volume of occurrences, and are flexible and responsive to react, and continuously adapt, to new suspicious patterns and activities.

The IBM® Counter Fraud Management and Improper Payments for Government solution is designed to help agencies avoid the 'pay and chase' scenario by intercepting transactions in real time that are potentially fraudulent, while detecting, identifying, and building the case against past fraudulent activity and improper payments. Looking at counter fraud operations as an entire lifecycle, this IBM solution introduces advanced analytics and investigative analysis throughout the entire process. Implementing this holistic approach allows agency staff to more effectively manage case workloads, optimize business processes and target high probability areas for fraud and abuse, thereby driving greater compliance and enhanced service to those citizens worthy.

A paradigm shift on how Health and Human Services agencies can combat fraud

Traditionally, observation spaces for agencies have existed in silos. Valuable sources of analytic data reside in many different system silos in a government organization, such as healthcare, social services, justice, public safety and community agencies. The business units operate and manage fraud vertically with point solutions. Relevant data is not shared and records are incomplete.

These silos create critical intelligence gaps within the organization. Suspicious activity and fraud patterns can remain undetected. In addition, disconnected and niche fraud solutions increase overall operating costs and resource needs.

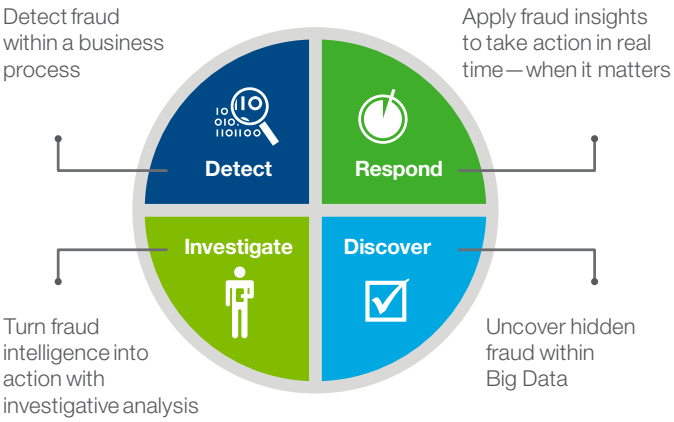

Figure 1: The IBM Counter Fraud Management and Improper Payments Solution for Government takes an enterprise approach.

The IBM Counter Fraud Management and Improper Payments helps bridge these gaps by building an ecosystem of tightly woven capabilities that use big data and entity analytics to eliminate information silos, expand the observation space, and enable unified enterprise business intelligence. Designed for the lifecycle of tracking and resolving fraudulent activity, IBM Counter Fraud Management and Improper Payments delivers strong insights that enable proactive and anticipatory decision making within the four operating components of detect, respond, investigate and discover (See Figure 1). It meets the needs of all agencies, and provides investigators, caseworkers and auditors with the ability to harness a deep set of unique analysis capabilities.

Operating components

Detect: Determine the accurate identity of an individual through analytic models, scoring and rules. Utilize intelligence from past discovery and investigation processes to recognize fraudulent activity patterns and highlight potential payment submission improprieties for further investigation by the investigations team.

Respond: Confidently differentiate legitimate submissions while preventing, or interrupting, suspicious actions by responding immediately to criminal patterns, activities, and intentions. A quick response deters criminals from pursuing further.

Investigate: Perform and manage the detailed inquires into suspicious activity that will support the compilation of evidence and provide the thorough analysis required to build more compelling cases for prosecution and recovery, or denial of payment. Leverage an established governance process for validating new rules, models, and watch lists that are crucial to the feedback loop in the fraud management lifecycle, helping to address dynamic changes in fraud schemes.

Discover: Leverage a rich set of analytic capabilities to identify non-compliance by retrospectively reviewing historical data, analyzing patterns and anomalies to identify individuals or organizations that might be developing fraud schemes.

IBM Counter Fraud Management provides a holistic, end-to-end approach

IBM Counter Fraud Management and Improper Payments delivers all components in one, advanced fraud solution for the agency. A wide variety of users, including case workers, program managers, agency directors and fraud investigators, will customize the data as needed. Robust dashboards provide a concise, overall view of the fraud management process. System reports enable analysis of existing and potential exposures and the effectiveness of current procedures. Ad-hoc and alerts are readily available to further improve decision making.

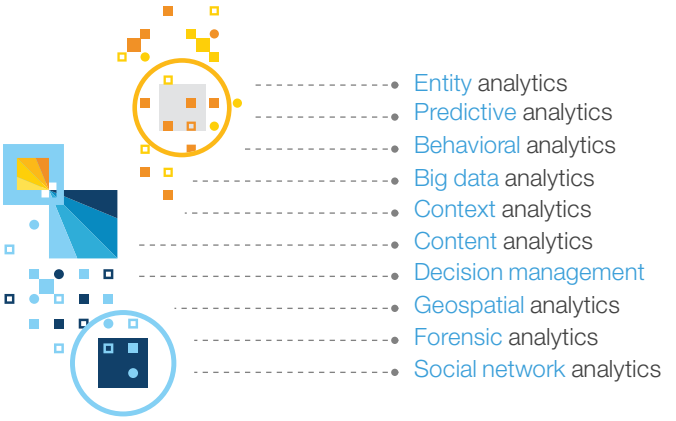

Figure 2: The IBM Counter Fraud Management and Improper Payments for Government offers rich analytical and decision-making capabilities.

Users can also proactively assess the impact of changes to operations and productivity. Visualizations depict contextual correlations that help team members gain deeper fraud insights. IBM Counter Fraud Management and Improper Payments employs multilayered analytical techniques throughout the observation space. Rich analytics extract insights, develop actionable intelligence, and invoke automated response capabilities using leading market analytics tools, as listed in Figure 2.

Improper submissions and fraudulent schemes are continuously evolving. Agencies must stay vigilant, constantly monitoring and adjusting their models and responses. Merging individual rules, analytics, and techniques into a seamless, end-to-end operation will enable the organization to have deeper insight and react with more confidence.

With IBM Counter Fraud Management and Improper Payments, government agencies can proactively combat fraud, reduce improper payments, improve investigator productivity while maintaining citizen confidence and trust in the program's integrity.

For more information

To learn more about IBM Counter Fraud Management and Improper Payments, visit **ibm.com**/smartercounterfraud or, contact your IBM representative.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
May 2014

1 Organization for Economic Co-operation and Development (OECD) (http://stats.oecd.org/Index aspx? DataSetCode=SOCX_AGG).

Please Recycle

GDS03002-USEN-00