WHITE PAPER

Reducing Government Budget Deficits by Attacking Fraud, Waste and Abuse

sas
THE POWER TO KNOW.

Contents

Fraud, Waste and Abuse Cost Governments Billions

All government programs are vulnerable to fraud, waste and abuse — now more than ever. Government fraud is at an all-time high and growing rapidly. Industry research shows that altogether, fraud, waste and abuse represent about 10 percent of overall government program spending.

Given the current fiscal crisis across the US and many other governments and ministries, no one can afford these kinds of losses. It's making budget deficits even bigger than they need to be — and forcing elected officials to close deficit gaps by either raising taxes or eliminating programs. Neither option is popular with voters.

But what if governments could minimize deficits by eliminating fraud, waste and abuse? It's an often overlooked way to close budget deficits — and one that forward-looking government leaders are already acting on by implementing enterprise-level, state-of-the-art fraud detection programs designed to keep pace with increasingly sophisticated perpetrators.

Understanding the New Nature of Fraud

The fact is, the nature of fraud has changed dramatically in recent years — largely because fewer government processes and data are paper-based. The advent of computerized systems has created a fertile environment for would-be perpetrators to access government systems and data and then use it to anonymously exploit government programs for personal profit.

Increasingly sophisticated in their ability to detect and circumvent traditional control measures, fraudsters use the internet to operate 24/7 and conduct fraud from foreign jurisdictions without extradition treaties. They are highly organized, patient and collaborative, often acting in collusion to attack multiple programs for maximum financial gain. And they are continuously updating fraud strategies to stay one step ahead of authorities — and may even engage insiders to understand the latest detection environment of government agencies.

Traditional Fraud Detection Methods Aren't Enough

Given the new nature of fraud, traditional program-focused methods of detecting fraud are insufficient. Modern-day fraud activities often span multiple departments, making fraud an enterprise problem — not just a program-specific problem. Programmatic approaches to fraud are designed to address individual programs, as illustrated in **Figure 1**. Because each program area may have its own fraud unit and fraud detection capability, the overall result is a very siloed approach to fraud detection and prevention, rendering governments unable to connect the dots to identify individuals and networks committing fraud across multiple program areas or systems. And without an enterprise view of data, investigators and analysts are limited in their ability to fully discern the complete risk exposure for any given entity.

The US Government Accountability Office (US GAO) estimates that improper payments hit $127 billion in 2014, up more than 17% from 2013.[1]

Each year the UK government loses an estimated £21 billion to fraud and improper payments, which is about 3% of total government spending.[2]

The US Office of Management and Budget (US OMB) reports that for 2015, 9.8% of all Medicaid payments were improper.[3]

The US Department of Labor estimates that $3.38 billion was paid improperly in the Unemployment Insurance program in 2015, a rate of more than 10.2%.[4]

In 2015, 12.1% of all Medicare Fee-For-Service payments were improper, totaling more than $43 billion, according to the US OMB.[5]

According to the U.S. Department of Agriculture, $2.8 billion in improper benefits were provided by the Supplemental Nutrition Assistance Program (SNAP) in 2015.[6]

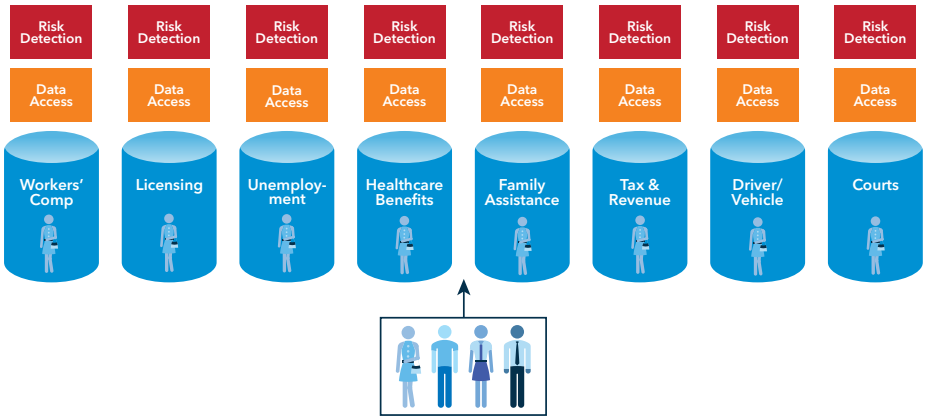

Figure 1: Siloed data access and fraud detection within and across government agencies prohibit an enterprise approach.

At the root of the problem are:

- **Poor data integrity:** Agencies have historically not shared data. By failing to integrate and validate data from various agency sources, data is often incomplete and unreliable – allowing fraudsters to fall through the cracks.
- **Siloed, disparate systems:** Agencies can only act on their own transaction or entity-level data, which means that they lack the broad set of enterprise data needed to put the transactions in proper context or detect cross-program fraud. Even when entity data has been pulled together into a data warehouse, it's usually not well-integrated, and it may not provide the holistic view of entities needed to uncover fraud-indicating patterns across departments and programs.
- **Limited analytic capabilities:** Agencies tend to rely on a narrow set of rules and basic analysis to detect fraud – leaving investigators at a significant disadvantage to modern fraudsters who utilize state-of-the-art schemes and technologies.

These blind spots make agencies susceptible to organized crime and illegal or unethical practices. They also leave agencies stuck in a reactive – rather than a proactive – position because they find out about fraudulent activity after damage has been done.

The Solution: An Enterprise Approach to Fraud

Spotting fraud early and moving aggressively to deal with it requires an enterprise fraud strategy. As illustrated in **Figure 2**, an "enterprise" approach is characterized by the fact that it:

- Eliminates data silos and provides a holistic view of data across programmatic and departmental boundaries.
- Helps coordinate fraud detection and interdiction efforts across all agency programs and departments.
- Detects and handles fraud alerts at the enterprise level so that anti-fraud efforts can be prioritized based on the overall egregiousness and value at risk for each entity being investigated.

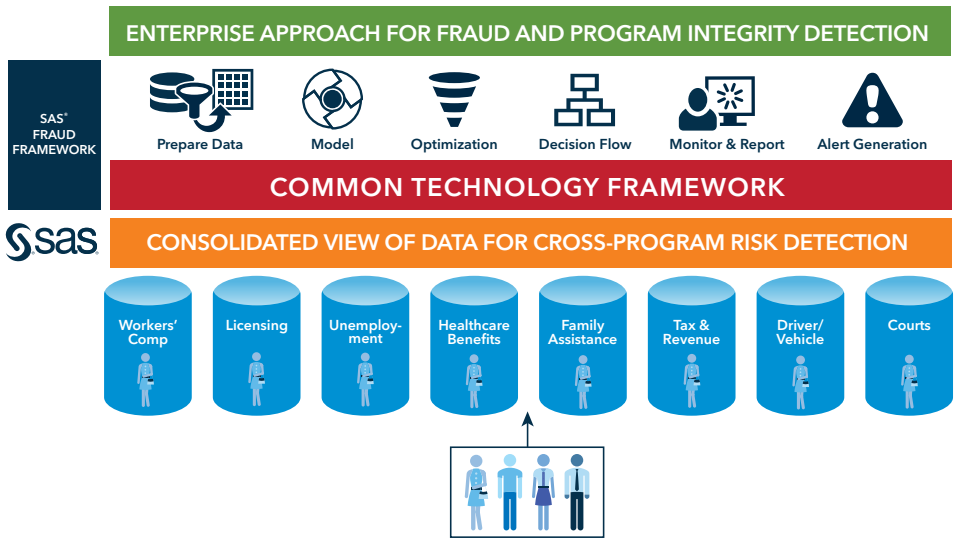

Figure 2: Taking an enterprise approach provides an integrated view of data and coordination of fraud detection across government programs through a common technology infrastructure.

To implement this strategy, governments need technologies that deliver several vital capabilities. To start, you need common access to enterprisewide data. For both automated detection and investigation purposes, access to enterprise data is crucial to uncovering previously hidden fraud patterns and increasing investigation efficiency – allowing more fraud to be exposed, investigated, and recovered or prosecuted without requiring additional staff.

Equally important, because fraudsters often intentionally provide inaccurate, incomplete or inconsistent information to prevent records matching across disparate systems, you need solutions that support entity resolution. The ability to disambiguate entities across multiple government programs and systems is paramount to creating a holistic view of program participants to identify aberrant behaviors.

Once access to enterprise data has been established, a sophisticated analytics approach is required to sift through the data and identify high-risk entities and transactions. As illustrated in **Figure 3**, this approach includes:

- Rules to mitigate known fraud schemes and detect program policy violations.
- Anomaly detection of individual and aggregated abnormal patterns.
- Predictive models that "learn" from known fraud occurrences and discover similar patterns as they emerge in the future.
- Social network analysis to identify suspect relationships such as collusion, aberrant referral patterns and organized fraud rings.

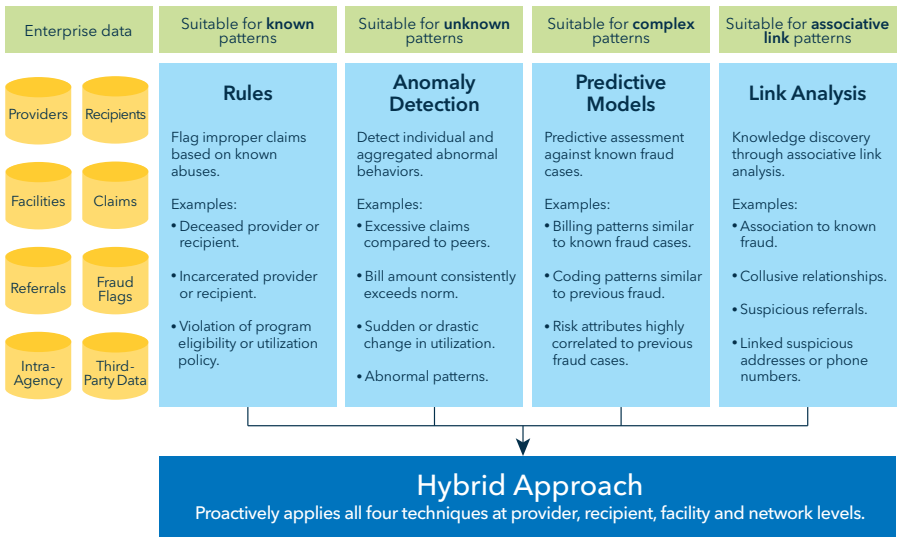

Figure 3: The best practice: A hybrid analytics approach to fraud detection.

But the need for cross-organizational communication doesn't stop with an alert regarding a rule violated or an anomaly detected. Responding to large-scale fraud threats may require the cooperation of multiple agencies and departments. That's why you also need a common case management framework that facilitates better collaboration and intelligence sharing between various departments and functions. Case management solutions can also provide complete case tracking and auditing from initial lead generation through to the ultimate disposition of every case.

And finally, governments need a single framework, or common application infrastructure, for developing fraud applications so they can reduce the time and expense required to deploy them, as well as free fraud staff so they can focus on the application rather than learning new tools and recreating the underlying environments.

Together, these capabilities – as part of an integrated enterprise fraud framework – make it possible for government fraud detection teams to:

- Gather and cross-match fraud-relevant data from all program areas, organizational units and geographic regions.
- Analyze this data to connect the dots and spot large-scale fraud attacks early in their life cycles.
- Prioritize alerts based on the level of risk that they pose to the entire enterprise.
- Plan and execute focused countermeasures to combat large-scale attacks.
- Develop and support highly skilled and motivated fraud teams who can carry out these tasks quickly and efficiently.
- Have more effective, efficient enterprisewide fraud detection and prevention that lowers associated costs.

The Benefits of an Enterprise Approach to Fraud Detection

By taking an enterprise approach to fraud, governments can boost the effectiveness and efficiency of their fraud detection efforts. For example, they can:

- Look at fraud holistically across the enterprise to identify large-scale fraud threats (such as organized and collusive fraud rings committing fraud or abuse across multiple programs) early in their development.
- Detect fraud earlier and more accurately because investigators can analyze complete, enterprisewide data to better classify participants and detect abnormal behaviors.
- Mount effective countermeasures while there is still time for them to have maximum impact.
- Save time by operating more efficiently – for example, by using tools that automate activities, focus on real prospects rather than phantoms and empower investigators to do more with less.
- Allocate resources more effectively – for instance, by focusing investigative resources on the highest-value cases.
- Increase the recovery of funds.
- Drive continuous improvement by feeding knowledge about the latest fraudulent activity into analytical models.
- Lower costs through economies of scale – by using a single platform that gives everyone access to centralized enterprise data quickly and easily. (In contrast, if investigators have to take a programmatic approach, they have to manually pull data together every time.)

Overcoming Barriers to an Enterprise Approach to Fraud

So what's holding governments back from implementing an enterprise approach to fraud detection? Often, they struggle to address technical issues, such as how to integrate their massive volumes of data and disambiguate entities to provide a holistic view of program participants across government programs and systems.

Government agencies also need to comply with complex laws and regulations regarding program operations, as well as those concerned with data privacy and confidentiality. High-profile data breaches have resulted in a public that is highly sensitive to how personal data is used and protected.

In addition, cultural barriers may limit the sharing of information across government departments and programs. Operating as unofficial "fiefdoms," various programs may be reluctant to share data, sometimes citing legal or regulatory restrictions that may be valid for only certain pieces of information rather than the entirety of their data.

However, these and other barriers are gradually being addressed by governments around the world. For example, in the US, many states are passing legislation to require secure and reasonable sharing of information between departments and programs.

These laws are being complemented by technologies that can integrate data across disparate systems and programs, giving investigators a holistic view of entities across all government touch points. And finally, continued global economic challenges are shifting the culture of government agencies so they no longer tolerate fraud that occurs because of lack of cooperation between government departments.

How SAS Can Help

SAS provides an enterprise approach to fraud with the SAS® Fraud Framework, which uses SAS software to support a three-pronged approach to fraud detection and prevention. This framework includes:

- A holistic view of entities that aggregates and integrates data from many sources and creates a solid foundation for rapid, comprehensive analysis.
- Sophisticated, hybrid analytics for powerful fraud detection and prevention.
- Easy-to-use interface that allows investigators to quickly identify, assess and act on leads and alerts based on seamless access to enterprise data.

As illustrated in **Figure 4**, the SAS Fraud Framework sits on top of the SAS technology platform, which encompasses SAS' data management, analytics, reporting and business solutions. And by layering on additional program-specific modules, the SAS Fraud Framework can be applied to many areas of government – from detecting collusive patterns in entitlement programs such as Medicare and Medicaid to purchase-card fraud, bid-rigging and terrorist financing.

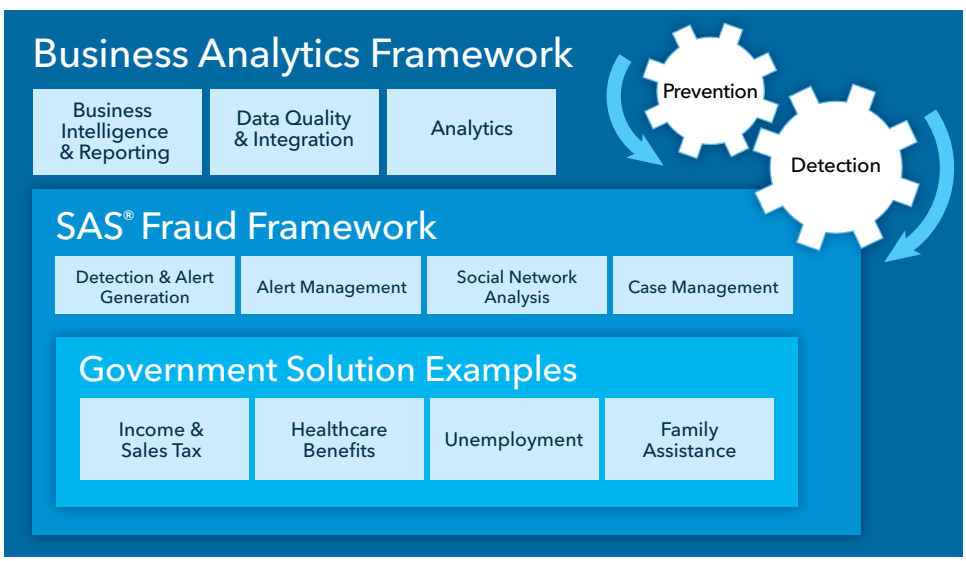

Figure 4: The SAS Fraud Framework can cover many government areas with a single, integrated solution.

How It Works

Working behind the scenes, integrated SAS analytical applications quickly connect the dots across programs in a variety of ways. Each "strand" of analytically determined connections represents another way of looking at any given fraud event as part of a potentially much larger threat. In this way, the applications in the SAS Fraud Framework work together to:

- Provide strategic insight into threats, trends and risks.
- Deliver a holistic enterprise view of fraudulent behavior.
- Rapidly test, simulate and deploy models/rules without dependence on IT.
- Support pre-payment detection and prevention.

As illustrated in **Figure 5**, the SAS Fraud Framework supports an integrated workflow for analyzing enterprise data and detecting potential fraud in near-real time. Data from a wide variety of operational data sources is aggregated to create a single, clean view of data that's optimized for fraud analysis:

- On the left of Figure 5, data from a wide variety of sources is integrated, centralized and cleansed.
- Data is then fed into the SAS Analytics engine for risk analysis and alert generation.
- Results of analytics then appear in a user interface optimized for investigative efficiency with all pertinent information readily available to investigators and presented in an easy to consume manner (as shown in the lower right-hand box).
- Integrated case management allows for the tracking of all activities from initial alert or lead creation through to ultimate disposition, whether that be a recovery action, educational outreach or criminal prosecution.
- And finally, the "learn and improve" cycle allows the results of each investigation to be fed back into the detection engine so that it can "learn" from investigation outcomes, adapt to changing fraud schemes and increase detection accuracy over time.

SAS provides this solution to many government organizations around the world, either as on-site or hosted implementation models.

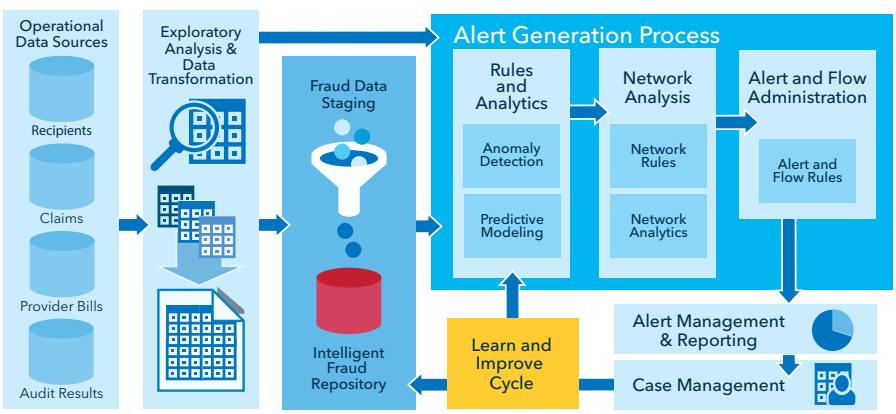

Figure 5: The workflow powered by the SAS® Fraud Framework integrated solution.

How SAS® Helps Government Agencies Detect Fraud Faster and Earlier

Improves data effectiveness

- A single version of the truth – along with sophisticated data matching and standardization routines, made possible by SAS data integration and ETL – reaches across multiple platforms, enabling critical decisions to be made more efficiently and with less risk.
- Using SAS for data quality lets organizations standardize and augment data while identifying duplicate names, addresses and other identifying information, and automatically resolve entities and entity relationships across multiple disparate data sources.

Improves audit and investigation effectiveness

- Proactively uncover undetected fraud patterns to identify and predict future risks with SAS' advanced analytical capabilities.
- Reduce false positives, maximizing recovery and prosecution resources while reducing processing time and recovery costs.
- Identify fraudulent claims before they are paid and prioritize investigation payments that seem likely to be improper.
- Focus on the highest-risk, highest-value cases through alert prioritization.
- Perform initial alert reviews in minutes rather than hours.
- Rapidly detect new fraud schemes and patterns before they cause significant losses.

Proving the Value: Customer Case Studies

The SAS Fraud Framework is a proven solution that's available today. Governments and ministries are already realizing tremendous returns on their investments.

National/Central Government

Like most national governments, the UK is losing a significant amount of revenue from tax fraud – about £15 billion a year. To combat this problem, HM Revenue & Customs (HMRC) is investing £917 million and anticipating a return of £7 billion in additional tax revenues. And with this effort, high-performance analytics plays a vital role.

Using SAS tools as part of the larger HMRC "Connect" system, HMRC can now bring together numerous internal and external data sources to reveal hidden relationships, and take investigative action much sooner and with much more efficiency. "Being able to react quickly and deal with extremely large data volumes is the key," says Bill Cockerill, a Data Analyst at HMRC.

SAS analytics and the HMRC Connect system improve tax fraud and evasion detection rates, provide opportunities for broader prevention, and create a deterrence effect – helping the government avoid significant losses and achieve higher tax revenues.

Local Government

In the US, Los Angeles County has been challenged recently by an increase in fraud related to child care services. The county estimates that fraud has grown by about 40 percent and, in many cases, is perpetrated by highly organized fraud rings. "We needed a unified approach to get a handle on the fraud problem," says Manuel Moreno, Director of Research at the county's Chief Executive Office. "We wanted a solution that provided data integration, as well as a powerful analytical tool workbench. To perform sophisticated predictive modeling, we needed historical data, and for that we had to integrate many external and internal data sources, such as the state of California's Employment Development Department data and business license data from Los Angeles County."

Los Angeles County selected the SAS Fraud Framework to address these challenges. Based on metrics developed in a controlled proof of concept, Moreno and his team concluded that data integration, social network analysis, predictive capabilities, data mining tools and the insight provided by the SAS solution can be used effectively to detect fraud before it occurs. "We calculated that the accuracy rate of fraud rings identified by the social network analysis solution to be, with reliability, 85 percent." In addition, the county expects a return on investment between $7 million and $30 million annually.

State Government

A US state is deploying a SAS enterprise system for fraud and improper payments detection across several state agencies, departments, institutions and programs. The system, which will be hosted at a SAS data center facility, will use a common infrastructure and a common set of data integration points across multiple program areas, providing a faster and more comprehensive fraud prevention regime at minimal cost to the state. For example, the state will use it to detect fraud and

improper payments in several health and human services programs, labor and workforce programs, and revenue and tax collections.

Identifying possible fraud or abuse at an early stage will alert state agencies and prevent them from making payments or releasing funds inappropriately, thus providing potentially millions in cost savings to the state. This state expects to realize $50 million in cost savings in the first year using the new system.

Learn More

To protect the fiscal condition of government agencies providing needed benefits to citizens, authorities must incorporate anti-fraud strategies and detection tools that place fraudsters on the defensive. SAS is uniquely positioned to team with our government partners to make this happen. The SAS Fraud Framework provides an end-to-end framework for detecting, preventing and managing all types of fraud and improper payments. Only SAS combines all of the approaches outlined in this paper in a single integrated, commercial-off-the-shelf software offering.

Furthermore, SAS is universally recognized as the worldwide leader of advanced analytics. Market share in predictive modeling alone is more than double our closest competitor. Only SAS can provide governments and ministries around the world with open, high-performance and scalable solutions for implementing analytics as part of an enterprise fraud detection strategy – providing both pre-payment prevention and post-payment detection capabilities across all public sector programs and services.

To learn more, visit SAS Fraud and Improper Payments.

Endnotes

[1] Addressing Improper Payments and the Tax Gap Would Improve the Government's Fiscal Position. GAO-16-92T, United States Government Accountability Office, October 1, 2015.

[2] Eliminating Public Sector Fraud: The Counter Fraud Taskforce Interim Report, UK Cabinet Office, National Fraud Authority, June 2011.

[3] Payment Accuracy Reporting, High Error Program Results for Medicaid, US Office of Management and Budget, 2015.

[4] Benefit Accuracy Measurement State Data Summary, Improper Payment Measurement Information Act Year 2015, United States Department of Labor.

[5] Payment Accuracy Reporting, High Error Program Results for Medicare Fee-For Service, US Office of Management and Budget, 2015.

[6] Payment Accuracy Reporting, High Error Program Results for Supplemental Nutrition Assistance Program (SNAP), US Office of Management and Budget, 2015.

To contact your local SAS office, please visit: sas.com/offices