WHITE PAPER

Using Modern Analytics to Save Government Programs Millions

Enabling an Enterprise Approach to Fraud Detection Within and Across Programs

sas
THE POWER TO KNOW.

Contents

The Changing Face of Government Fraud

Massive fraud and improper payments remain a significant challenge for governments at all levels. The threat goes far beyond individuals making false statements to get more benefits. Today, organized crime rings develop sophisticated schemes and tools and go after state and federal governments much like bank robbers – by looking for "soft" targets with little security and weak controls so they can quickly get away without being detected.

Whether these attacks are "smash and grabs" of large sums from one program (for example, they offer a free walker to an elderly person, use this to get their Medicare data, then heavily bill against it for fraudulent items or services) or stealing small amounts through improper payments across multiple programs, fraudsters are shockingly successful today. Each year, the states and federal government lose billions of dollars due to fraud and abuse of benefits. Besides seeking out easy targets, the most successful fraud rings commit fraud in smaller amounts from multiple programs, so their actions never appear as an outlier on one program data set with rules-based analytics.

In most cases, the result is a pay-and-chase game that yields little in return, especially when perpetrators create corporations or limited liability companies (LLCs) to make and receive improper claims and payments. Typically, they commit fraud, dissolve the company and then disappear. It's very difficult to use the legal system to "break the corporate veil" and attach debts to the individuals who once owned a now-defunct LLC. Put simply, the game board is tilted in the favor of fraudsters under the pay-and-chase approach to fraud detection.

Attacks Now Occur Within and *Across* Programs, Increasing the Potential for Losses

High-profile examples of government fraud abound – and the incremental costs add up quickly (see sidebar). For example, according to the federal Office of Management and Budget, for fiscal year 2017, improper payments reached all-time highs, including:

- $36 billion for Medicaid (or 10 percent of total expenditures) – a 27 percent increase over 2015.
- $1 billion for Children's Health Insurance Program – a 96 percent increase over 2015.
- $4 billion for unemployment insurance – a 17 percent increase over 2015.
- $237 million for child care (not including Temporary Assistance to Need Families or social services).[1]

Fraud numbers are so huge because fraud rings are not only getting more effective at what they do, but because they can easily target multiple government programs simultaneously. Whereas in the past, fraudsters tended to focus on exploitation of one government program, today the same fraud ring will steal from multiple programs – even if payoffs are small – just because they can. A provider may bill Medicare, Medicaid and other programs for the same services – and currently, it's unlikely that these programs share data in a way that makes it easy to detect fraudulent overbilling.

---

[1] https://paymentaccuracy.gov/resources/r

Given these new trends, investigators need to take an integrated approach to detect and address fraud so nothing falls through the cracks. To better understand why, consider three real-world scenarios:

- A convenience store that takes food assistance benefits uses electronic benefit transfer. The owner rings up $125 in groceries and provides the cardholder $75 in cash instead, known as food stamp trafficking. The storeowners underpay their taxes by failing to report the trafficking proceeds and abuse the lottery with the unreported cash. This single case encompasses food stamp fraud, wire fraud, tax fraud, lottery fraud and money laundering.
- A child care center may be billing for services not provided and submitting electronic claims – possibly with a swipe card. This center may also hire low-skilled employees from public assistance roles to obtain tax credits from the Department of Labor workforce programs. Once hired, these employees often need subsidized child care, which the employer can easily provide. If the employee doesn't want to work, the child care center just bills for services not provided and gives the employee a small kickback, disguised as wages, to stay home with their own children.
- A home health agency may also bill for services not rendered and "hire" fake employees from public assistance roles to secure tax credits. If the new employee has a Medicaid card, it won't be long before billing occurs for home health services for family members. If the fake employee can recruit others with Medicare and Medicaid cards, they may get kickbacks.

Now, what if one person, or small group of people, owned and operated all these businesses? Just like the walls between these shady businesses, there are virtual walls between different government programs. Most fraud investigators only work within their own program silo. Even if staff from one program found fraud, they would likely miss fraudulent activities against other programs.

What's Holding Fraud Investigators Back?

The question is, why aren't governments successfully detecting cross-departmental threats?

As the prior example illustrates, criminals use their ingenuity and flexibility to take advantage of the government's inability to connect the dots between state, federal and local government databases. Regulatory constraints and privacy concerns – especially at the state level – may even prohibit investigators from mixing siloed data sets and viewing them holistically. In addition, professional criminals regularly change tactics and serially open and close business locations; if these businesses are protected by the corporate veil of a legal entity like an LLC, it's even harder for investigators to attach recoveries to owners of defunct stores and health care providers.

Equipping Investigators for Success With an Enterprise Approach to Fraud Detection

Given these challenges, fraud investigators need next-generation analytic tools that cut across data and program silos and empower government investigators to go on the offensive with fraud operators – without disrupting the efficient and timely delivery of benefits, services or tax refunds. Ideally, these tools support an enterprise approach to fraud detection by:

- Centralizing diverse data sets from across government programs in a single benefit database while ensuring data quality.
- Analyzing this data holistically to identify abnormalities, trends and hidden patterns indicative of potential fraud.
- Calculating the propensity for fraud at each stage of a process with a fraud analytical engine that uses multiple analytic techniques – powered by the latest innovations in AI/machine learning – to detect fraud in the first few months of a crime ring's operation.

This approach, as shown in Figure 1, enables governments to break down silos and pool data from various programs before analyzing it in breakthrough ways to detect fraud much earlier – before payments are sent. For example, social network analytics powered by machine learning can spot relationships across government programs and efficiently identify patterns in the millions of rows of data – something that humans simply can't do effectively. To return to our earlier example, it makes it possible to spot $500 food assistance fraud early, shut down the fraud ring, and prevent the multimillion-dollar, cross-program health care fraud perpetrated after this initial crime.

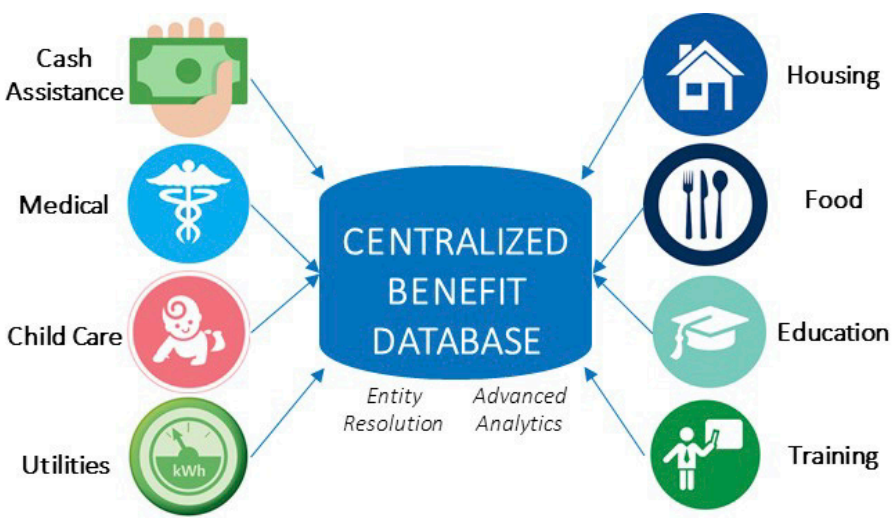

Figure 1: SAS® pools data from across system and program silos and analyzes it to detect fraud earlier.

Let's examine the technical capabilities you need to successfully operationalize government fraud detection and investigation that short circuits the pay-and-chase cycle.

Data Integration and Quality Management

To be accurate, advanced analytic and AI/machine learning algorithms need:

- Centralized data.
- Data of sufficient quality.
- The links between data sets identified.

Ideally, you want data from a wide range of related sources, as advanced analytics and AI can use it to find integrity and fraud issues faster and earlier. Unfortunately, many older government systems still use rudimentary rules and outdated technology platforms to support benefit program operations, and their data is typically fragmented and of poor quality. Poor data quality hurts BI data analysts focused on fraud in terms of budgeting, rate setting, reporting, program results analysis, and tracing the root cause of program and fraud issues. (This same data issue also hurts program integrity data analysis.) In addition, if more than half your data is bad, the algorithms will learn the wrong trends and ultimately provide you with inaccurate results.

AI and ML can't fix these large-scale data issues – they can only identify anomalous data and reflect it as outliers. But data management combined with the right advanced analytics and AI/ML can ensure high data quality and integration across diverse data sources – and ultimately deliver a true end-to-end solution.

Automated Business Rules

Fraud investigators use logic – based on their experience and acquired best practices – to understand data and systematically analyze it to detect fraud. Automated business rules apply the logic that fraud investigators already know in order to drive faster, earlier, more effective fraud detection. Because automation vastly increases efficiency, it enables you to analyze all your data – not just sample sets – so nothing gets overlooked. Data from multiple programs can be combined to get an enterprise view of fraudulent activity.

Ideally, fraud detection software includes a business rules management system that governs and automates the logical statements needed to support repeatable, accurate fraud detection decisions. Given how quickly fraud is evolving, it should also provide a way to consistently manage those rules. This is especially important in health care, where programs process millions of claims each month.

Predictive Modeling

Predictive modeling involves the use of data mining, analysis and probabilities on historical data in order to forecast potential outcomes. The goal is to go beyond knowing what has happened to providing a best assessment of what *will* happen. These models can be a simple linear equation or a complex neural network mapped out by sophisticated software. As new data is added to the predictive model, it's either validated or revised to further improve accuracy.

Predictive models are vital to helping government agencies detect fraud. Combining multiple analytics methods can improve pattern detection and prevent criminal behavior. As cybersecurity becomes a growing concern, high-performance behavioral analytics can examine all actions on a network in real time – relative to historical data and patterns – to spot abnormalities that may indicate current or future fraud, zero-day vulnerabilities and advanced persistent threats.

Search and Discovery

New fraud schemes are being created all the time. While automation and alerts allow you to maximize the efficiency of fraud investigators and program integrity staff, they still need the ability to dive into the data themselves. This requires a toolset that empowers them to follow their hunches, explore ideas and look for new patterns in data indicative of cross-program risk.

Network Link Analysis

Network link analysis is a powerful tool in the fraud detection toolbox, especially because of its ability to drive data visualizations that make the invisible visible. For example, data visualization software can pull all the targets, claims and sites together in a cluster in seconds. This is incredibly powerful from an anti-fraud perspective because it enables an investigator to pull a thread on the potential fraud detected and watch a much larger and complex fraud scheme come unraveled instantly.

Artificial Intelligence (AI)

Artificial intelligence is the science of training systems to emulate human tasks through learning and automation. It enables a machine to learn from the massive volumes of data it ingests to identify patterns and relationships that exist within the data itself. AI systems can then extract key features, determine a method of analysis, write the code to execute that analysis and produce an intelligent output through an automated process – all with minimal intervention, but substantial influence, from human counterparts who couldn't begin to complete this much work in a fast and efficient manner. With AI, people can have the equivalent of 10,000 human brains working simultaneously, augmenting what fraud investigators are doing. This frees them to focus on the most important alerts and ensures investigative staff provide maximum value to your organization.

One type of AI is machine learning – a method of data analysis that automates analytical model building. It is a branch of AI based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention. Because machine learning often uses an iterative approach to learn from data, the learning can be easily automated. Passes are run through the data until a robust pattern is found. These patterns can then be used to detect fraud in large and complex data sets. This enables deep learning and insights, reveals patterns in data that are normally invisible – and answers the questions you didn't even know to ask.

These AI and machine learning technologies can be incorporated into your existing systems to refine existing fraud detection models – for example, by:

- **Combining historical data with artificial intelligence to build new models and detect anomalies that require extensive connecting of diverse dots across vast sets of data**. In practical terms, this means enabling fraud analysts to take the models they already have, since they know they work, and make them better. This makes the fraud analysts and investigators partners in implementation and use of the new system. They know the data better than anyone else, and they can provide insight to the data scientists building new models and algorithms so the machine helps make them better at what they do.
- **Optimizing the capabilities of AI in detecting anomalous claims earlier in the process to reduce the pay-and-chase and move toward cooperative fraud prevention**. This is particularly valuable when it comes to improper payments, because fraud is designed to make these improper payments look real to the systems paying them. On the surface, they look good, so it's not the fault of the people who run the payment system that fraudulent payments are made. In fact, they need to pay the more than 95 percent of claims that are real in a timely manner. To prevent fraud in this case, governments need both a payment system and high-quality fraud detection tools.
- **Interjecting a fraudulent flag at the time of the eligibility check for members prior to service being rendered**. This can be accomplished by utilizing each member's historical validated data to formulate a dynamic, AI-driven user profile.
- **Identifying the social determinants of poor health outcomes** – the structural determinants and conditions in which people are born, grow, live, work and age that are linked statistically to poor health care outcomes and compliance. Interestingly, the same tools that can fight fraud can be used to assess and drive health care quality. When health outcomes are poor, it can lead to poor quality of care, which statistically leads to fraud, waste and abuse. Fraud investigators can use AI and ML to reverse-engineer health outcomes and detect fraud.

SAS: Delivering an Enterprise Approach to Fraud Detection and Investigation

SAS® Detection and Investigation for Government delivers all these technical capabilities to enable:

- Data integration and business rule deployment and management.
- Search and discovery.
- Advanced analytics, machine learning and AI, and model deployment.
- Fraud detection and alert generation.
- Alert management.
- Social network analysis.
- Intelligent case management.
- Hosting and analytical services.

As a result, your investigative teams can use advanced analytics and AI to detect and prevent opportunistic and professional fraud. They can standardize, integrate and authenticate data and consolidate program integrity activities. And because SAS Detection and Investigation for Government provides a single, end-to-end framework that uses multiple techniques – predictive modeling and AI, anomaly detection text mining, network link analysis, automated business rules – investigators can identify fraudulent activity and stop payments before they are made. At the same time, precise targeting dramatically reduces false positives, ensuring that the vast majority of valid transactions are processed without delay.

Applying the Best of AI, Machine Learning and Automation to Transform Fraud Detection

SAS has built AI and machine learning capabilities into the very foundation of SAS Detection and Investigation for Government, enabling a next-generation approach to fraud detection. These capabilities enable government investigators to identify abnormalities and patterns that may indicate fraudulent activity – for instance, by finding patterns and aberrations using visualization and analysis techniques. SAS calculates the propensity for fraud at each stage of a process with a fraud analytical engine that uses all these techniques to enable the following critical activities.

SAS and AI: A Rich History

SAS has had a stake in the AI game since the company was founded in 1976 – from early work with neural networks in the '70s, to classical and modern machine learning in the '80s, '90s and 2000s to present-day innovations in deep learning. Today, SAS offers a wide range of modern machine learning algorithms and base capabilities suitable for AI applications, including machine and deep learning, computer vision, natural language processing, and forecasting and optimization, among others. These capabilities are used to predict, classify or detect important patterns in data and abnormalities in images.

For businesses looking for an AI partner, no other solution provider offers the same level of automation, governance, deployment expertise and trust as SAS.

As shown in Figure 2, SAS advanced analytics – powered by AI and machine learning – enables fraud investigators to move from a traditional approach of identifying fraud to an advanced, enterprise approach that enables faster, earlier fraud detection and prevention.

Old Approach	New Approach
Investigator receives memo, email or call to review a claim	Investigator logs into system and picks up new alerts, allocated cases and today's tasks
Starts desk research to pull together information on claim from systems and files	Provided with a single view of known information and clickable visualization
Manually searches external data sources to build case	Easily builds case - workflow ensures thorough process
Looks to build out network of other parties and associated claims	Template investigation plans maintain quality and facilitates tasking
Pulls everything together and can now start field investigations	Automatic generation of reports including money saved

Figure 2: SAS transforms how fraud investigators work – and helps them find fraud faster and easier.

Whereas before, investigators get bogged down with manual requests, data aggregation and data searches, SAS Detection and Investigation for Government vastly streamlines the fraud investigation process by empowering them to:

- Intake all available data from across programs and pull it into a single platform, seamlessly and automatically, to evaluate every potential fraud case, every time.
- Use machine learning to rapidly develop advanced models to identify outliers and hidden patterns in data.

- Build social networks, visually connect providers together and identify member networks.
- Apply deep learning to building models – and swiftly create new models to stay ahead of evolving fraud schemes.

This transformed detection and investigation process enables governments to:

- Detect fraudulent activity earlier and more precisely.
- Apply machine learning and AI to detect previously unknown schemes and spot linked entities and crime rings.
- Reduce fraud losses by detecting repeat offenders and insider and collusive behavior – and thus prevent fraud before payments are made.
- Reduce the costs to detect and investigate fraud by minimizing false positives and improving investigative efficiency and ROI per investigator.
- Gain a consolidated view of risk to improve models as fraud trends evolve and new threats emerge.
- Improve transparency and increase accountability by accurately measuring, not estimating, improper payment rates over time and building easy-to-understand models.

SAS at Work: State of Illinois Tackles Health Care Claims Fraud With SAS® Analytics

To illustrate the power of SAS Detection and Investigation and SAS Visual Investigator, consider the following case study of the state of Illinois. In recent years, the Inspector General's Department of Healthcare and Family Services transformed its Medicaid program using SAS Analytics to identify overpayments and prevent further improper payments to health care providers.

Weishin Wang, Assistant Bureau Chief and Project Manager, says the agency needed a solution that would do more than just rely on exception-processing runs to compare providers to their peers. It wanted to use insights from existing integrity review audits to generate future fraud case referrals – discovering fraud at the transaction or patient level, as well as uncovering fraud perpetrated by members of criminal networks.

The underlying fraud platform, based on SAS, uses historical data on previous fraud and abuse cases to develop well-honed fraud predictors. By utilizing the insights from known fraud cases, the system can spot provider collusion and identify undiscovered fraudulent providers and criminal networks – avoiding significant fraud-related financial losses each year.

"From the past, when we suspect an individual or provider of fraud, we go through an assessment study to understand the case," explains Wang. "The process has always been lengthy and requires significant human resources to identify the initial referral issue. Our predictive models were based on supervised and unsupervised Medicaid claims information by using SAS analytical tools to orchestrate the provider risk score index table. We are still finalizing our predictive model, but test results have so far proved that it can successfully direct us to targeted providers. Furthermore, we have customized comprehensive routines, with interrelated patient information, to identify suspicious networking activities among providers.

> With this modeling approach, our accuracy is much, much higher... We've also decreased the time to create a model from weeks to just a few hours.
>
> Weishin Wang, Inspector General's Department of Healthcare and Family Services

"We can identify fraudulent activity, such as time-dependable billing issues, non-corresponding medical claims and double billing, and decide whether to refer the cases to law enforcement agencies, terminate their status and potentially recoup the claim funds. Our approach looks at identified providers and variables to create a pre-modeling base of patterns. We then apply a model to the entire list of member providers to score and identify previously unknown cases of fraud. Even with cautionary patterns identified, we don't approach the provider until we model the social network aspects of an individual. By combining the score from each model, we have a stronger indication of fraudulent behavior to investigate.

Looking at data at a very detailed level and finding interrelations through social networks is what Wang calls a DNA (dynamic networks association) routine, which provides the proof that a provider is acting in a fraudulent manner. "With this modeling approach, our accuracy is much, much higher – we've achieved a very prominent accuracy level," he says. "We've also decreased the time to create a model from weeks to just a few hours."

Wang says the agency chose SAS because of its ability to access, integrate and manage data from multiple sources, allowing the agency to run analytics against the data and then share that information instantly throughout the organization. "Sometimes people can't believe what we find," he says. "SAS has a tremendous manipulation capacity, and it is unbelievably more efficient in generating and distributing reports than any tool I have ever used."

Benefits

- Identified overpayments and prevented further improper payments.
- Uncovered criminal network fraud.
- Avoided significant fraud-related financial losses.
- Decreased time to create models from weeks to a few hours.
- Reporting efficiency.

SAS: Evolving Solutions to Keep You One Step Ahead of Organized Fraud

Federal, state and local government agencies providing subsidies to citizens and legal immigrants must place themselves on the offensive by incorporating strategies and tools that make it risky to commit fraud. SAS is uniquely positioned to team with federal agencies to make this happen. SAS Fraud Detection and Investigation provides an end-to-end framework for detecting, preventing and managing all types of abuse of federal subsidies and loan programs. Only SAS combines all the approaches outlined in this paper in a single, integrated, commercial-off-the-shelf software offering, providing improved efficiency and decreased total cost of ownership in implementing these capabilities.

Learn More

SAS is universally recognized as the worldwide leader of advanced analytics. SAS' market share in predictive modeling alone is more than double its closest competitor's. Only SAS can provide government programs with an open, high-performance and scalable solution for implementing analytics throughout your fraud detection strategy at the point of eligibility screening and provider and vendor enrollment, prepayment within the benefit payment system, or in post-payment review.

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