An Enterprise Approach to Fraud Detection and Prevention in Government Programs

Featuring:
Greg Henderson, Government Practice Principal
SAS Fraud and Financial Crimes Practice

Carl Hammersburg, Senior Solutions Architect
SAS Government Fraud
# Table of Contents

- **Introduction** ............................................. 1  
- **Why Traditional Fraud Control Systems Are Not Enough** ........... 2  
  - Silo Systems With Inadequate Data Sharing .......................... 2  
  - Limited Analytic Capabilities ...................................... 3  
- **An Enterprise Approach to Fraud Detection and Prevention** ....... 4  
  - Business Analytics Framework ..................................... 4  
  - Fraud Detection Framework ......................................... 5  
  - Government-Specific Modules ....................................... 5  
- **A Closer Look At Hybrid Analytics** ............................... 6  
- **Barriers To Adopting An Enterprise Approach** ..................... 8  
  - Cultural Barriers .................................................. 8  
  - Technical Barriers .................................................. 8  
  - Regulatory Barriers ................................................ 10  
- **Lessons Learned** ........................................... 10  
- **Closing Thoughts** .......................................... 11  
- **About The Presenters** ....................................... 11  
- **For More Information** ......................................... 12
Introduction

A 47-year-old Montana woman was sentenced to 27 months in prison for fraudulently taking more than $115,000 in food stamps, housing assistance benefits, Medicaid and Supplemental Security Income (SSI) benefits.

A pharmacy operating out of a Miami-area storefront billed Medicaid for nearly $800,000 in a matter of days. The perpetrators turned out to be veteran fraudsters. One was already facing state charges for staging auto accidents in an insurance scam; the other was a suspect in another case involving a fake clinic and nearly $400,000 in improper payments.

Government agencies face enormous challenges in trying to prevent improper payments resulting from fraud, waste and abuse. The US Office of Management and Budget estimated that the government lost more than $115 billion in improper payments in fiscal year 2011 alone – and that’s probably a conservative estimate.

Whatever the cause of the improper payments – data entry errors, authentication and verification errors, or criminal intent – taxpayers end up footing the bill. Fraud also takes a toll on government programs themselves, which are subject to budget cuts, inadequate and reduced program funding, possible review by the Inspector General and other legislative bodies.

The examples above aren’t notable for the dollar amounts but for the fact that the perpetrators were operating across programs and channels, said Greg Henderson, Government Practice Principal in the Fraud and Financial Crimes Practice at SAS. Fraud is not always confined to a single program. “We’re seeing a broader trend where individuals are not just exploiting one program but operating across multiple programs.”

Similarly, a single type of fraud can affect multiple programs. For example, consider state unemployment insurance programs, many of which are borrowing billions of dollars from the federal government to keep operating. Fraud and abuse is rampant in this area; employee misclassification is a major concern. When an employer misclassifies employees as contract workers (reporting their earnings on a 1099 rather than a W2 form), the financial ramifications extend to several programs. There is typically no withholding or coverage for unemployment insurance, workers compensation, disability insurance, or state or federal income taxes. All of those programs feel the effects.

The challenges of detecting and preventing fraud are intensifying with the growing sophistication of fraudsters’ strategies. “In the past, the majority of fraud and abuse has been of an opportunistic nature,” said Henderson. “Now the perpetrators are much more professional, sophisticated and organized. We are no longer just looking at a single individual using a single channel to exploit a single product in a single exposure. We are now dealing with professional criminals who are working with other criminals. They know what our internal controls are. They plant or engage insiders to help them circumvent those controls, and they simultaneously target multiple program areas, products and channels.”
Why Traditional Fraud Control Systems Are Not Enough

“The racketeers, drug smugglers and bank robbers of the past are now moving into professional white collar financial crimes, including fraud – and that has caused a dramatic shift in how we need to detect and prevent fraud,” said Henderson. “The systems and controls of the past were very well tuned to dealing with that opportunistic individual; it takes more sophisticated tools to deal with organized fraud rings and collusion.”

In trying to combat fraud, government agencies are constrained by inadequate data sharing and limited analytic capabilities.

Silo Systems With Inadequate Data Sharing

“The various government programs are often run by completely different groups, each with its own audit, investigations and compliance functions,” said Henderson. “These groups generally don’t work well together in identifying fraud and abuse – or in sharing that information with other groups so they can follow up accordingly.” As a result, agencies can act only on their own transaction- or entity-level data. They lack the broad set of enterprise data that could put the transactions in proper context or detect cross-program fraud.

“Fraud units and systems are not necessarily structured around John Doe the citizen, and how John Doe interacts with all of our products and programs through the various interaction channels,” said Henderson. “We end up with a silo situation where data about John Doe is spread out across the entire organization. That data is potentially very valuable, because the more I know about John Doe, the better I can determine whether or not his behaviors are appropriate.”

Even when entity data has been pulled together into a data warehouse, it’s usually not well integrated. An informal poll of the webinar audience confirmed this deficiency. When asked how well their organizations use enterprise data assets for fraud detection and prevention, more than half of respondents gave their organizations low ratings. There is clearly room for improvement.

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.

“Government organizations are typically structured around individual programs or products. They’re not necessarily structured around John Doe the citizen, and how John Doe interacts with all of our products and programs through the various interaction channels.”

Greg Henderson
Government Practice Principal, Fraud and Financial Crimes Practice, SAS
An Enterprise Approach to Fraud Detection and Prevention in Government Programs

State Government Programs

Investigative Unit
Fraud Detection System
Data Access
Workers Comp

Investigative Unit
Fraud Detection System
Data Access
Unemployment

Investigative Unit
Fraud Detection System
Data Access
Medicaid

Investigative Unit
Fraud Detection System
Data Access
TANF

Investigative Unit
Fraud Detection System
Data Access
SNAP

Investigative Unit
Fraud Detection System
Data Access
TAX / Revenue

Investigative Unit
Fraud Detection System
Data Access
DMV

Investigative Unit
Fraud Detection System
Data Access
Courts

Investigative Unit
Fraud Detection System
Data Access
Corrections

Figure 1: Silo systems prevent governments from gaining a much-needed holistic perspective.

Limited Analytic Capabilities

Agencies tend to rely on a narrow set of rules and basic analysis to detect fraud, while the fraudsters are using complex schemes and state-of-the-art technologies. “If we’ve been exposed to a certain fraud scheme, we may put a business rule in place that will help us detect that scheme in the future,” said Henderson. “Those business rules are actually very good at detecting known fraud, but they typically have hard thresholds associated with them, which are pretty easy for fraudsters to discover. Fraudsters can then operate just under the radar and avoid detection.”

Furthermore, fraudsters are continuously updating their strategies to stay one step ahead of authorities. They may even engage insiders to understand the latest detection environments. As a result, agencies tend to operate in a reactive mode, discovering fraud only after the damage has been done.

When each program area has its own fraud unit and fraud detection capability, governments cannot connect the dots to identify individuals and networks committing fraud across multiple program areas or systems. 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.
An Enterprise Approach to Fraud Detection and Prevention

Spotting fraud early and moving aggressively to deal with it requires enterprise-level vigilance and context. The concept of an enterprise approach acknowledges the fact that John Doe exists across program areas – and calls for a common infrastructure foundation that supports that broader view. The foundation for this common infrastructure is a business analytics framework – overlaid with a common fraud detection framework and supplemented by government modules for specific programs, such as Medicare/Medicaid, tax evasion and law enforcement. A common infrastructure foundation enables governments to more quickly and effectively detect fraud, at lower cost.

Enterprise Approach

Modular Approach

Business Analytics Framework

The first piece of this common infrastructure is a data management foundation that provides access to data across programs, products and channels. It doesn’t require a database overhaul or a massive central data warehouse, but rather a data integration layer that can source from databases around the organization – and from external public or purchased data. Because fraudsters often intentionally provide inaccurate, incomplete or inconsistent information to prevent records matching across disparate systems, you need data quality capabilities that support entity resolution.

The business analytics foundation also provides a variety of analytics to identify patterns that could point to fraud, and the business intelligence and reporting mechanisms to deliver meaningful information to investigators.

Figure 2: The enterprise approach is based on a common business analytics framework overlaid with a common fraud detection framework and modules for specific government programs.
Fraud Detection Framework

The second component of the common infrastructure is a set of tools and utilities that support the work of investigative staff, including:

- A common detection engine that can look across all the data sources to identify aberrant behaviors and bring them to investigators’ attention.
- Tools that enable special investigation unit (SIU) investigators to drill into underlying detail data to triage alerts and support investigations, case workflow and ultimate disposition.

“A lot of investigators spend inordinate amounts of time logging into multiple systems to pull data on persons of interest as they’re doing investigations,” said Henderson. “In an enterprise approach, that data is pre-aggregated, consolidated and integrated, so investigators simply click on a series of tabs in a screen to get the needed information. They can then focus their time on investigation and analysis, rather than on gathering and manually integrating the data.”

Government-Specific Modules

An enterprise approach does not require a centralized SIU. SIUs can continue to be specialized by program area. Each agency or program can share the common underlying business analytics and fraud frameworks (with appropriate security and access controls), supported by purpose-built modules that reflect fraud patterns unique to each program area. With a modular approach on a shared foundation, it is much quicker and less costly to expand into new program areas, because you don’t have to reinvent the wheel or procure a new fraud program, just add a new piece to what is already there.

This layered infrastructure performs in a continuously improving loop, said Henderson. “The data is integrated and pumped into the detection engine, where we then apply analytics to the data to detect aberrant behaviors, which then generates alerts. Alerts pass to the investigative interface, where investigators can triage the alerts and, if warranted, send them to the case management system to facilitate the entire workflow associated with the case and its disposition.

“Since professional fraudsters have gotten very good at constantly changing their behaviors to stay ahead of fraud controls, we need to be able to constantly pump the results of investigations back into the analytics. When the analytics can adapt to the changing behaviors seen in transactional data, the system is continuously improving and produces fewer and fewer false positives and false negatives over time.”

“To keep pace with today’s fraudsters, it’s no longer enough to do ad hoc audits or investigations against the data. We need systems that continuously monitor the activity in transactional systems to look for aberrant behaviors and deliver them to investigators.”

Greg Henderson
Government Practice Principal, Fraud and Financial Crimes Practice, SAS

“Once you’ve got that underlying data foundation in place, it is much quicker and less costly to expand out to the next program area, because you don’t have to reinvent the wheel or procure another fraud program. It’s just a small, incremental set of work to add that next program into the enterprise architecture.”

Greg Henderson
Government Practice Principal, Fraud and Financial Crimes Practice, SAS
A Closer Look At Hybrid Analytics

As fraudsters get more sophisticated in detecting and circumventing traditional control measures, they can easily slip through fraud detection technologies that are based on business rules. Business rules are a good place to start, but a rigorous fraud detection engine requires multiple data and analytic techniques, often complementing each other.

Database searching and matching techniques identify discrepancies in behavior or information for an entity across multiple systems. For instance, it could identify a person who signs up for a welfare-to-work or child care subsidy program (for which one of the program requirements is to be employed), while also applying to receive other benefits intended for unemployed people.

Anomaly detection is very good at helping us know what we don’t know. Rather than looking for specific known fraud schemes, it looks for behaviors that are unusual or unexpected.

- **Historical anomaly detection** looks at an individual’s or entity’s changes in behavior over time. If the system sees a sudden, drastic shift from a historical pattern – with nothing else in the data to explain that shift – this would be flagged as an anomaly and factored into the overall fraud risk score for that entity.

- **Peer grouping or clustering** compare an individual’s behavior to the norm for a demographically similar peer group, and identifies individuals whose behavior is drastically different from what would be expected for that group.

  For example, consider two health care providers, each submitting $10 million worth of Medicaid claims. On the surface, those two providers and the claims could look identical, but what if the state’s tax records show that one provider reported $150,000 in net revenues while the other reported $150 million? What if the state licensing agency reports that one provider had three licensed physicians and five nurses, while the other has 100 physicians and 200 nurses? Taken in fuller context, it’s easy to see which provider’s Medicaid claims fall out of normal parameters.

Text mining identifies patterns in unstructured data, such as reports and social media. In a fraud detection context, text mining could be useful for unearthing factual discrepancies, scripted words or phrases, or phrases indicative of lying.

With advanced analytics such as predictive modeling, you can build models that identify attributes or patterns that are highly correlated with known fraud, even complex and emerging patterns of fraud. The models are then used to score incoming transactions to determine if they look more like known fraud or more like known valid transactions. Those scores factor into the overall risk score associated with the entity.
As fraud evolves more toward organized fraud rings, social network analysis identifies relationships among entities, based on static attributes in the data (phone numbers or addresses, for example) or transactional attributes, such as referral relationships. For example, the SAS Advanced Analytics Lab created a custom solution that enables an automobile insurance provider to better identify fraudulent claims. The system identifies staged accidents or false claims by finding suspicious patterns or overlaps in relationships, such as cases where an individual is the insured party in one case and a passenger in another, or where the insured party and claimant have the same phone number, or where there is repeated use of the same body shops and medical professionals.

“A broad variety of analytical techniques can be applied to identify aberrant behaviors,” said Henderson. “By using multiple techniques in combination, we can cast a very wide net. The techniques provide checks and balances against each other, and using multiple factors to calculate a composite fraud score at an entity level helps reduces false positives, so the system does not generate alerts that consume investigators’ time without action being taken.”

Figure 3: Using multiple analytic techniques to calculate a composite fraud score identifies fraud that would otherwise go undetected and reduces false positives.
Barriers To adopting An Enterprise Approach

Anyone who has worked in government knows that getting agencies and IT systems to work together is easier said than done. The merits of an enterprise approach seem self-evident, but there are cultural, technology and regulatory barriers to overcome.

Cultural Barriers

Cultural barriers inevitably limit the sharing of information across government departments and programs. “Frankly, fraud isn’t on the forefront of everyone’s mind,” said Carl Hammersburg, Senior Solutions Architect for Government Fraud at SAS, who worked in state government for 20 years. “You’ll often get the pushback that fraud control is not a ‘core’ agency function. I spent many years feeling like we were the red-headed stepchildren before the agency came around and we used a much more enterprise-focused approach.”

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. To help make the case for cross-agency data sharing, don’t focus on the word “fraud,” which can get a negative reception. Use studies and examples to show how information sharing can advance the agency’s core mission and help resolve the agency’s pain points, such as budget shortfalls, tax gaps or return on investment. Point out how an enterprise approach can help the business areas be more timely, efficient and effective in their work.

“If there hasn’t been a legislative or executive-level push to put together an enterprise approach, promote the idea based on value in return,” said Hammersburg. “What can you provide from within your organization’s own data that will help that other program or agency succeed in its mission? In one case, I found we just didn’t have the data the organization needed, so we brokered a conversation with a third agency to get them pulled in, so everyone could find something of value.”

Technical Barriers

It can be a real negotiation coup to set in place appropriate Memoranda of Understanding (MOUs) that specify how interagency data sharing will take place. “If you have a contracts section, partner with them early,” Hammersburg advised. “Have the conversation started with the agencies so you know there’s a data-sharing possibility there, and then get those contracts folks to understand what you’re trying to do and how you’re trying to do it. Then they can be a good advocate partner rather than a barrier later in the process.”
Organizations all have their own preferred formats for contracts and MOUs; don’t let the format become the sticking point, said Hammersburg. “In my work with state government, one of our contracts with the US Department of Labor was only two pages, very simple yet broad in terms of the data we could share. It even allowed for joint enforcement possibilities. On the other hand, we had a 20-page contract with our state unemployment agency that went into excruciating detail about which fields from which systems would be shared, who could receive the data, how training would be done, the auditing process and so on. Either type of MOU can work, as long as it reflects the core issues of what each party wants to gain in the end.”

The information technology (IT) platform can be another barrier – or at least a perceived one. In a world of legacy mainframe systems and incompatible databases, it can seem like data sharing would be an idealistic vision. Not so, said Hammersburg. “For what we were doing at the state and federal levels, flat file transfers through secure FTP usually sufficed.”

When you get that data, don’t get hung up on discrepancies at the individual record level. Focus more on where there is strong data quality and where there are weaknesses. For entity resolution, start with trying to look for hard matches, but consider the technology to do some “fuzzy matching.” Fuzzy matching can be particularly helpful when working with businesses, because there may be many people associated with one business and many businesses associated with one person.

“In doing entity resolution across systems, go with the identifier that works the best,” said Hammersburg. “When we were matching up with our state’s general tax agency, we had a common identifier at the state level. For the federal level, we needed to use the federal employer ID number (FEIN). This was the best identifier to match up, but we knew that our own FEIN numbers weren’t that good. So we matched with the state’s general tax agency, pulled in their FEIN numbers, and then matched that up with the IRS. That really helped us triangulate around it and do a good job pulling it together, even though we knew that we had some data quality issues.”

Similarly, you’ll need to understand when different terms are used for the same thing, or when the same term has different meanings across agencies or programs. Doing the work upfront to establish a good data dictionary will prevent you from pulling the wrong data together and creating a garbage-in-garbage-out result.

Finally, there are concerns about security. What restrictions apply to the data and what protections are required? Can the information be freely shared or does it have to reside on a dedicated server in a locked cage in your locked data center? “Make sure you know the data restrictions up front, so you don’t violate the terms of use,” said Hammersburg. “Apply role-based security to control data access, but don’t lock the data down any tighter than necessary, because the consolidated information can be useful for business areas other than fraud control.”

Organizations often struggle with 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. These barriers are real but not insurmountable.
Regulatory Barriers

Government agencies need to comply with complex laws and regulations regarding program operations, particularly related to data privacy and confidentiality. High-profile data breaches have resulted in fines, jail sentences, and a public that is twitchy about how personal data is used and protected.

As you ask agencies to share their data, it's important to be able to distinguish "can't" versus "won't," said Hammersburg. "I was regularly told by lots of different people, ‘We can't do that; the law prevents us from doing that.’ And what I invariably found is they might have misinterpreted the law or the person had been misinformed. So I finally got to the point of saying, ‘Great, show me exactly where that is.’ Often they couldn't find [the regulation], or if they could find it, it wasn’t as restrictive as they thought."

When working with highly restricted data, such as data governed by HIPAA and PII protections, make sure you understand the limitations, train staff on the barriers to use and consequences of misuse, and consider writing these provisions into your MOUs and contracts.

What if you discover something that could be useful to another agency, but you can't directly hand them the information? You can tip them off to where some valuable information can be found, and let them get it through their own MOU with that agency, Hammersburg noted.

Lessons Learned

Hammersburg shared some lessons learned about implementing an enterprise fraud approach, based on two decades in state government.

**Once may not be enough.** “You’ll get through these cultural, technical and regulatory barriers one time and think it’s all over, but it won’t be,” said Hammersburg. “For example, you’ll have to amend MOUs to address unforeseen circumstances, such as an IT vendor coming in to work on your core systems and potentially being able to see the data. The MOUs will expire and need to be renewed. Every single time one of those expiration dates came up with our unemployment agency, I had to fight the battle again with somebody new, explaining our need for the data, how we’re going to use it, and so on.”

**Connect with the business area.** “You’re going to be linked up with someone who will give you the signoff to use the data, but typically that person is more interested in protecting the data than in granting access to it,” said Hammersburg. The best way to win them over is to show how they can gain business value from data sharing. “For example, when we were pulling together a master system based on the tax issues we were trying to solve, we became the number one source of audit leads for the unemployment agency and a significant source of audit leads for our general tax agency.” Mutual benefit is a great way to garner support.

“If you’re providing data to another agency, make sure they’re using it and are successful with it,” said Hammersburg. “If they’re finding value in your data, they’ll be much more interested in sharing theirs.”

Carl Hammersburg
Senior Solutions Architect, Government Fraud, SAS
Closing Thoughts

With a true enterprise view of fraud through a single entity view, a government can:

- Eliminate data silos and provide a holistic view of data across programmatic and departmental boundaries.
- Help coordinate fraud detection and interdiction efforts across all agency programs and departments.
- Detect and handle fraud alerts at the enterprise level so that antifraud efforts can be prioritized based on the overall egregiousness and value at risk for each entity being investigated.

“The economy and the budget situations in state governments have created a change in mindset, where it’s not acceptable to treat fraud, waste and abuse as a cost of doing business,” said Henderson. “Fraud represents a fairly large cost, around 10 percent of the budget, by some estimates. When you consider a typical state budget, you’re looking at anywhere from $1 billion to $2 billion of fraud, waste and abuse. If you could prevent or recapture that, it would go a long way toward closing the budget gap.

“So the mindset today, compared to five years ago, has really changed. We’re seeing a lot of legislation being passed and executive orders coming out of governors’ offices to break down the barriers. The real key to making fraud, waste and abuse a top-of-mind issue among senior leadership is to focus less on the criminal aspects and more on the financial impacts. Once senior officials in an organization realize the scope of loss that’s occurring, that really gets their attention. And they have the authority and the will to effect that change.”

About The Presenters

Greg Henderson
Government Practice Principal
SAS Fraud and Financial Crimes Practice

Greg Henderson develops and supports the company’s global strategy related to addressing government fraud, improper payments and noncompliance issues.

Henderson has nearly 15 years of experience in fraud and financial crimes in both the public and private sectors and has been at the forefront of the development of SAS solutions for banking fraud, anti-money laundering and terrorist financing. Most recently, he assisted in developing an enterprise approach to fraud detection and prevention in the public sector.

Henderson is a published author of several papers, is a frequent speaker at industry conferences and has provided legislative testimony on fraud and financial crimes.
Carl Hammersburg
Senior Solutions Architect, Government Fraud
SAS Fraud and Financial Crimes Practice

Carl Hammersburg joined SAS in early 2012 after spending 20 years in anti-fraud activities for Washington state’s exclusive workers’ compensation insurer, the Department of Labor and Industries. In 2004, Hammersburg formed that agency’s comprehensive fraud program, covering premium tax audits, claim investigations, provider fraud and collections. Data-sharing and investigative partnerships with other state and federal agencies, as well as driving public availability of information and awareness, served as cornerstones to the program’s anti-fraud activities.

Under Hammersburg’s stewardship, audit and investigative activities doubled and outcomes tripled, based on a focus on data mining and predictive analytics that improved efficiency and case selection. Program success under his leadership drew awards from two successive governors of Washington state. In his final year with the state, the program collected more than $148 million, with a return on investment of more than $8 for every $1 spent.

For More Information

White Paper
Reducing Government Budget Deficits by Attacking Fraud, Waste and Abuse
sas.com/reg/gen/corp/2089667

On-Demand Webinar (conducted in partnership with the ACFE)
Hiding in Silos: Leveraging Disparate Data to Detect and Prevent Fraud
sas.com/reg/web/corp/1199423
About SAS

SAS is the leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Through innovative solutions, SAS helps customers at more than 60,000 sites improve performance and deliver value by making better decisions faster. Since 1976 SAS has been giving customers around the world THE POWER TO KNOW®. For more information on SAS® Business Analytics software and services, visit sas.com.