Paper 322-2011

Why Government can Lead in Fighting Fraud, and use Social Networks and the SAS® Fraud Framework to get there

Carl Hammersburg, Washington State Department of Labor and Industries

Abstract:

The Washington State Department of Labor and Industries has built a state-of-the art tool for detecting and preventing workers' compensation premium fraud, based upon the SAS Fraud Framework and Social Network Analysis. This paper details the history of our path, and the broader opportunity for government institutions to take a leadership role in fighting fraud.

Background:

For too long, fraud, and the effort to combat it, was treated as an ancillary activity by most organizations, public and private. A taboo topic to discuss publicly, it often became taboo within the organization as well.

While private companies have a critical focus on the bottom line regardless of their line of products or services, government institutions are not normally tasked with the same viewpoint. Typically underfunded for their core missions, government agencies are often punished for under spending even those meager allotments, resulting in a disincentive to "leave money on the table". While those agencies at times provide services at a lower cost due to the lack of building in profit as well as the lack of need for advertising or sales budgets, they are tasked with core missions, such as providing public health, income assistance, unemployment insurance and job training, that do not include fighting fraud as part of that core mission.

Spending money on resources to investigate, audit and collect from people or institutions, as well as pursue cases criminally often strikes managers as a diversion of thin resources from the core mission they have been tasked with. Exceptions include agencies such as the Internal Revenue Service and many state revenue departments, with sole missions to bring in taxes at an appropriate level.

At the same time, the public is increasingly skeptical of government, and suspicious of whether money is spent wisely. Huge fraud rings are occurring on a regular basis, particularly evident within Medicaid and Medicare, but happening across all programs and agencies, on both the revenue and spending side. Those facts bring many to believe that government agencies at all levels are not good stewards of the taxes that come from the hard-earned money of companies and individuals.

In 2004, the Washington State Department of Labor and Industries set off on a public path to fight fraud and abuse in our workers' compensation system. To do so involved the need to deal with premium tax fraud on more than $1.1 billion in premiums from

176,000 companies each year, as well as battle fraud from claimants and medical providers. The agency did this in response to surveys and focus groups from our customers and policy holders. As a monopolistic market, they did not have the option of moving their business, and they spoke up loud and clear, stating that fraud was their biggest concern, and they felt we were horrible at dealing with it.

Since that time, the battle against fraud has become one of our core agency goals. We tackled the problem through a series of actions that included new legislation, increased staffing, and replacing computer systems. But the real success comes from a core focus on detection and prevention. This has become a profit center for the agency, with an ROI averaging 8:1, even with increased spending.

Detecting and preventing fraud starts with a robust system for detecting it. Our homegrown solutions in this arena have been a large part of a successful approach so far, but will not make us a leader. We have now partnered with SAS to build out a comprehensive system to detect abuse and fraud in workers' compensation premiums by employers. The SAS Fraud Framework had the most robust set of tools to put our broad range of data to work actively saving money.

Private companies compared to government – advantages versus disadvantages

Many corporate institutions have taken the lead in battling fraud. In the retail and banking environments, this was once the battle for physical security, and to a lesser extent, counterfeiting. The front lines have shifted significantly regardless of industry. Losses due to identity theft are on the rise dramatically. The leveling power of the Internet has opened up institutions in countries with historically lower rates of fraud and corruption to organized rings established in countries with weak oversight. Transaction speed and volumes create huge risks at the same time as they have opened opportunities.

Corporations and other private entities have many advantages when it comes to fighting fraud. Their budgets are limited, just as within government, but have more room for variance, and willingness to spend on an area that can bring a greater rate of return and improve the bottom line for shareholders. The ability to compare an ROI for fraud detection and prevention efforts with other internal rates of return on capitol allows for an opportunity to determine the most effective level of spending in this area. In order to leverage CRM opportunities, just-in-time inventory and online transactions, most successful players in many industries have already invested heavily in modern computer hardware and software.

Additionally, private companies have a greater opportunity to influence who is in their customer base, and exactly how much product is going to them. Particularly on the taxing end, governments rely on voluntary reporting first and foremost, meaning they don't even know how much they should be collecting. It is difficult to imagine SAS in an situation where they don't know how much they should even be billing a customer. Services can also be cut off much more quickly if fraud is suspected, without as many legal hurdles in most cases, or rounds of appeals. Removing a bad doctor or clinic from a

network for purposes of workers' compensation medical services, or accepting Medicaid or Medicare faces a much higher threshold.

Advantages that government institutions have may not seem apparent at first. However, looking deeper there are a number of them. The first is that government institutions can and will share their data broadly with their counterparts. This allows for a much fuller view of peoples and companies, and the inconsistencies evident in fraud come to light when strong data mining and proper predictive modeling is applied to that data. A second strength is the power of the solutions that many agencies have at their fingertips. Rather than bringing a lawsuit, they are able to move directly and quickly when they have delinquencies or uncover fraud. Remedies include filing tax liens, garnishing wages and seizing bank accounts. Those are all accomplished more quickly and at much lower cost than the remedies available to private citizens and companies.

While fraud against a government agency can be huge in terms of dollar volume, it typically happens over a longer period of time due to low transaction speed. This means that point-of-sale fraud detection, and its need for extremely high speed of processing is not an area of focus for most government institutions.

Unfortunately, surveys show an increasing percentage of the public in the United States that believe certain forms of fraud are unacceptable. Many individuals who answer that it would never be acceptable to shoplift from a retail store also state that they believe at least some level of fraud against insurance companies or government taxing agencies is acceptable. That is an uphill tide to fight. On the other hand, when an organization shows that it will investigate and take action, members of the public are willing to step forward to give tips on certain types of fraud. We are finding that as our efforts are publicized more, our toll-free hotline and Internet tip hits are increasing dramatically. Referrals for both potential claims fraud and employer premium fraud more than doubled in the past year alone. In some cases, it is competitors who know about another business in their industry that is committing fraud. Others include neighbors or family members who report an individual committing claims fraud.

While other motivations may be at work as well, often it is the connection between taxes and the fraud that drives the contact. The true costs of fraud may feel hidden to end consumers in many industries, particularly because corporations do not want to reveal it to them or their competitors, the public role of government and its discussion causes a different dynamic. Private individuals and companies realize it is their tax dollars that aren't coming in when taxes are cheated, or going out the door with benefit fraud, and in an increasing number of cases, that is compelling action. That is an advantage that many corporations do not have.

Solutions – the power of data sharing, complex analysis and the SAS Fraud Framework

Taking the lead in the fight against fraud begins with a fundamental shift in attitude from government agencies. As with our agency, those agencies must become very public in

admitting the problem and choosing to take it on. Early on, they will need to divert resources from their "core" missions in order to staff appropriately. Many have spent little or no resources on a comprehensive system for detecting fraud, instead throwing resources at the auditors or investigators needed to act on leads without actually building a network to develop those leads. That is exactly what Labor and Industries looked like less than a decade ago.

Despite the premise of this paper, that government has the opportunity to become a leader in fighting fraud and developing techniques to do so, ultimately, success lies in a public and private partnership. Underlying technology solutions that are needed in complex predictive modeling and analyzing social networks are best developed by private companies like SAS. Their experience in partnering with many of the largest players in the financial, insurance and medical industries has a direct translation to the types of fraud that government agencies face.

When Labor and Industries turned to a solution to move from a home-grown fraud detection system largely formed on rules and models to deal with outliers based on known fraud patterns, the SAS Fraud Framework stood out. Its abilities to deal with unknown and complex patterns, learning predictive models and social network analysis stood out. The power of the data held within our agency, such as wage and hour claims and investigations, safety inspections, construction contractor and licensing, as well as workers' compensation provided an excellent backdrop for advanced analytics. Adding to that data that we obtain through sharing agreements with the Internal Revenue Service, our state Department of Revenue, and unemployment insurance information provided a nearly unique data-set.

By focusing first on employers and workers' compensation premium tax fraud, we added a layer of complexity. Identity resolution for businesses looks far different than individuals, with flowing and inconsistent information across those many data sets. Building the appropriate rules up front to deal with many-to-many identity relationships and come back with a confidence score took time and effort from both expert modelers within SAS and our own business process experts. Extremely high controls around the data coming from the Internal Revenue Service also ensured that we had data cordoned off even within our own system.

While many elements of the SAS Fraud Framework have evolved over time, the full solution set is still in its infancy. Our project ran in parallel with an implementation with Los Angeles County in their Health and Human Services arena. Los Angeles County had completed a successful pilot that uncovered a huge fraud ring in its first hour of operation, representing a multi-million dollar potential return on investment.

As opposed to solutions that government agencies developed in the past, which tended to be overly customized, and couldn't scale and improve over time without another extensive IT project, operating with the SAS Fraud Framework represents a different form of solution. Many items are customized to our view of the work, with specific risk classifications for insurance premium calculation, a unique data set made of information

from other agencies, and our own fraud experience for modeling. However, at the same time, this is a software solution that will continue to evolve over time. Those enhancements come with the licensing, and are built on the same type of feedback from other SAS products. The community of expert users provide the feedback of what works and what doesn't, and ultimately, newer and better tools in fighting fraud continue to be built into the system. As an early member of that community, we have some of the heavier lifting that comes with being at the forefront, a position that government rarely has in the technology arena. In crafting our solution, many of our design goal were incorporated into the solution itself, ensuring that all future users can benefit from the same tools.

A hybrid approach to fraud analytics:

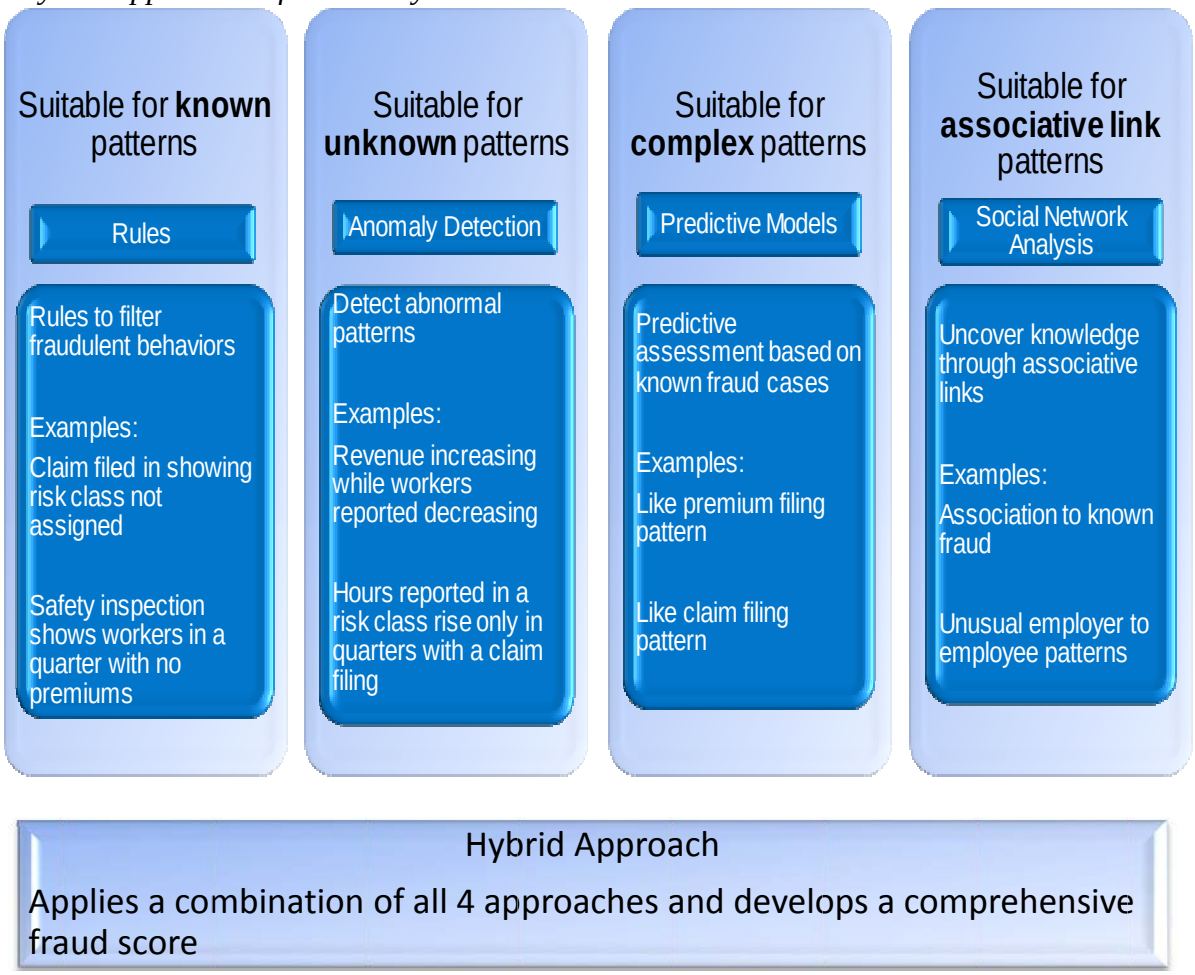

Figure 1

The hybrid approach built into the SAS Fraud Framework, and the method in which we implemented allows all four areas to run in parallel, and integrates those into a comprehensive fraud score. Tips and leads also receive scoring and are part of the ranked list that fraud detection screening staff review. False positives are removed, as are

employers that we do not want to review at this time for other reasons, including action taken recently that may not yet have affected future behavior.

Graphical display of the information greatly enhances the speed of screening staff, and any information they may want to review from dozens of different computer systems are all sorted and tabbed.

In the figure below, an example of the graphical nature of information displayed for staff is shown. This "tab" on a firm shows history of reporting by risk classification over time, with the weighted average displayed.

Risk classes that are less expensive in dollars per hour appear lower in the display, more expensive classes at the top. The size of each bubble reflects amount of reporting in that class in a given quarter, and a red ring around the outside reflects a claim filed by an injured worker in that class that quarter. A bubble that is not shaded in represents zero hours filed in that risk class.

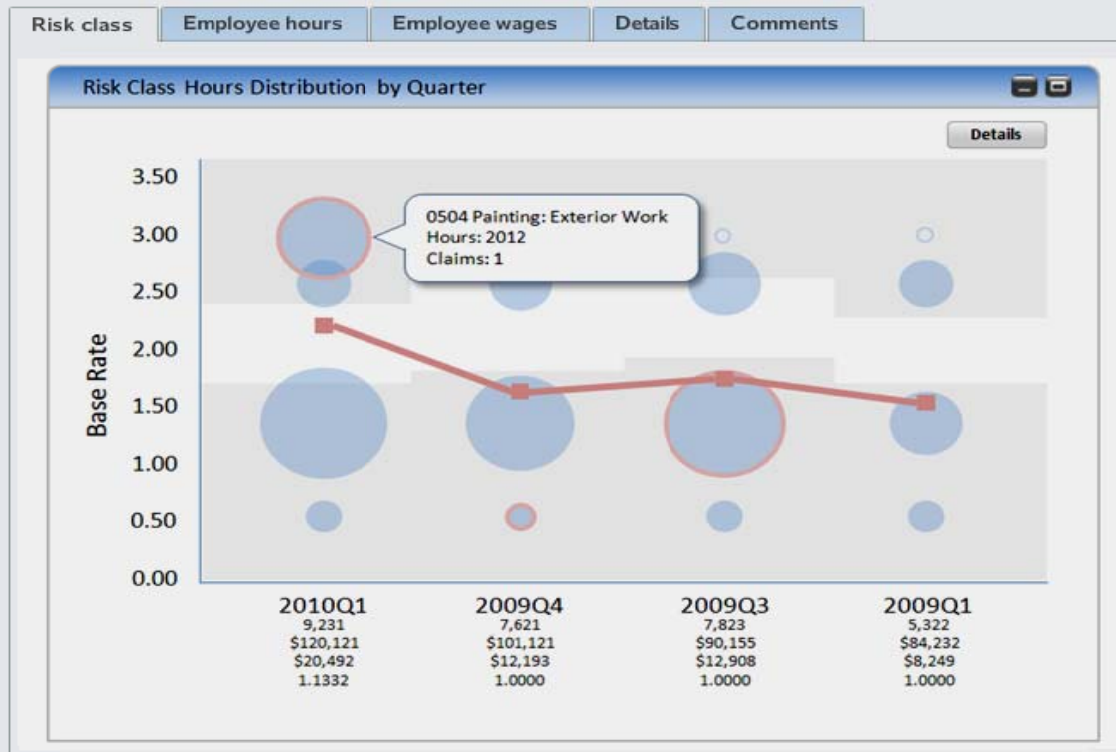

Figure 2

In this example, a claim happened in the first quarter of 2010 in the most expensive risk class. The firm also reported a significant number of hours in that class. A rules-based detection system would label this appropriate and move on. However, more complex analysis shows a pattern, with zero hours filed in the most expensive class for any quarter

where a claim was not filed. The system will flag and score this for fraud, and our staff can quickly see graphically what is happening.

Social media and social network analysis

Some of our more interesting and public cases these days are deeply embedded in the new world, where people increasingly open up their lives in various forms of social media, and everyone obtains at least their "15 minutes of fame".

One example is the story of Christopher Briejer, who we prosecuted and was convicted of fraud, a total of 56 counts of theft for workers' compensation benefits he wasn't entitled to. This case started with an anonymous tip through our website that led us to a video he posted on YouTube after climbing Mt. Rainier (above 10,000 feet), despite his claims that his back was too disabled to do any work.

In February of 2011, we arraigned James (Jimmy) Smith, of AxMen fame on the History Channel on 17 counts of theft. While that case has not gone to trial yet, our evidence of his ability to work while on a pension for workers' compensation all ran on prime time television. He is videotaped scuba diving and wrapping chains around logs while underwater, along with many other actions he was deemed too disabled to perform.

While these may be more extreme examples, cases are increasingly either proven, or at least discovered, by the intersection of government with new media and social networks. Cases are accumulating that involve information gleaned from MySpace, Facebook and other sources. Craigslist is becoming a regular source for us to find unregistered companies that are performing work.

Long-term opportunities exist by combining the power of data from within government and private databases with information put into the public domain by the individuals under potential investigation. Text mining of applications for key words, names and other indicators can cross-reference to build a database.

Not only is social media critical, but truly gaining insight into the "social network" of an individual or company. By knowing who they associate with, past and present, we can increase the effectiveness of predictive modeling, or identify a resurfacing of a known criminal or "bad actor" on the civil side very rapidly. That approach changes the fight against fraud from civil recoupment or conviction after the fact to proactive steps that can prevent the fraud from happening, or stop it very rapidly. At the same time, it changes the fight against fraud from dealing with one individual or company at a time to uncovering rings of fraud – whether organized criminal organizations, or simply friends, family or other extensions of social networks that learn how to model from one example.

Solutions – what else is needed?

Data-mining and a proper detection system provide the best return on investment and ensure that all other staff achieve the best return by focusing them on cases with the best

expected outcomes. At the same time, other tools are needed for government to succeed in the fight against fraud.

Privacy rules continue to battle against the fight to prevent fraud. A systematic lowering of barriers between agencies of the federal government, various states and local jurisdictions would provide the maximum information for all to succeed in lowering fraud and abuse. In many cases, barriers are more perceived than real. Many times in the last 6 years, I have questioned the answer when told that another agency couldn't share data with us to detect and prevent fraud. Many of those barriers have been overturned. Most just took willpower and managers on both sides willing to push back on perception or overly cautious advice from legal counsel.

Our state also passed a law specifically inscribing the ability of our three main taxing agencies, the Department of Revenue, Labor and Industries and Employment Security (unemployment) to share data, just to ensure that the barrier stays low. More will need to be done to change the laws to support this critical sharing of information. Just as the firewalls in place between policy and investigative agencies helped lead to the mistakes that happened with 9/11, leading to many changes afterwards, government tax and aid agencies have their hands tied in many ways.

A second legal challenge is the pull between the need for government to be open and broad in its services and allowing access for those that should be approved beneficiaries or vendors, yet prevent abuse and fraud. Dramatically lowering the threshold for discontinuing services or removing vendors from networks when substantial evidence of misuse is evident, without huge costs and long timelines of drawn out appeals will significantly shift the balance of power. In such a situation, the power of an advanced analytics system for detection becomes exponentially more powerful.

Lastly, incentives need to be broad based. The goal is for the public, private companies, liberals and conservatives in government and the government institutions themselves to all see the value. Some of this was evident in Washington State in recent years. A joint legislative task force with members of the Democratic and Republican parties, business and labor came together with representatives of key taxing and enforcement agencies. They publicly talked about the problems facing the construction industry, and passed a wide range of legislation that provided tools to improve the problem, as well as adding key resources to the agencies tasked with enforcement. While some of the legislation proved more partisan, many bills passed unanimously, or nearly so.

Ensuring that the benefits of fighting fraud are evident by tying them to increased funding support for the agencies that make those efforts, but also shared by publicly holding down tax rates for businesses and individuals will ensure that all come together to support the push.

SAS® is a registered trademark of SAS Institute, Inc. in the USA and other countries. Other products are registered trademarks or trademarks of their respective companies.