INTERNATIONAL
INSTITUTE FOR
ANALYTICS™

RESEARCH BRIEF
RESEARCH & ADVISORY NETWORK

An Enterprise Approach to Fraud Detection and Prevention in Government

GREG HENDERSON, Senior Director, Global Fraud and Security Intelligence Practice, SAS Institute Inc.

ROBERT MORISON, IIA Lead Faculty

SEPTEMBER 2015

A Fast Changing Landscape

Fraud and improper payments continue to be a pervasive problem in government agencies. Lately, organized crime, including offshore organizations, is becoming a bigger part of the problem. Identity theft is on the rise, some of it through cyber-breaches, and that sows the seeds for fraudulent claims and transactions. And as governments offer more services online as a convenience to citizens that creates opportunities for fraudsters to operate remotely and not have to present themselves physically to gain access to government benefits.

The problem is huge. Fraud and improper payment rates are estimated at 7-15 percent, varying by agency. Around $70 billion per year is lost within Medicare and Medicaid alone. People steal identities and file false tax returns under those names, maximizing refundable credits and deductions, and claiming refunds. Health care and tax fraud tend to grab the headlines, but every benefit program at every level of government is vulnerable to fraud, waste, and abuse. For example, employers avoid paying unemployment insurance taxes, and beneficiaries claim unemployment benefits they may not be entitled to when they are working under the table or fail to meet other eligibility criteria. Billions of dollars are spent on unemployment benefits at the state level, and often between 10-15 percent of that is improper payments. Other social benefit programs, such as child care subsidy and food assistance, are also vulnerable to fraud, but the dollar amounts are lower.

The problem takes different forms. The legal definition of “fraud” includes criminal intent. “Waste” means spending money that shouldn’t be spent on things that aren’t needed. “Abuse” is where providers or beneficiaries in government programs bend the rules and receive improper payments or benefits, but they do not meet the standard of criminal intent. A common example is the medical provider who exaggerates the services rendered, billing a 30-minute office visit as 60 minutes. But whether it’s technically fraud, waste, or abuse, government needs to care because it represents financial loss regardless.

To complicate the landscape further, fraudsters present moving targets. They are constantly evolving their schemes, so the nature of fraud is always changing. As soon as we identify a scheme and put in controls to mitigate it, the fraudsters very quickly find new ways to exploit the system. The organized criminal elements committing fraud against government programs are especially sophisticated. This is their job, and they take it very seriously. They are trained and adept at technology, and they know how things work on the Internet.

In short, fraud detection and prevention is a very dynamic environment. Governments need to become as sophisticated in their use of technology as the fraudsters are, and they need technologies that can adapt quickly to the changing nature of how fraud is being committed.

Financial Opportunity

Advanced analytics have been in use for fraud detection in the private sector, especially in financial services, for several decades. Through a proactive and aggressive approach, the industry has been able to reduce fraud rates to less than 0.5 percent. Government agencies have lots of room for improvement, and they are beginning to adopt some of the highly proven techniques in financial services to be able to detect fraud and potentially prevent it from happening in the first place.

Government agencies operate under continual budget constraints, but reducing fraud is an investment that pays off. When faced with deficits, governments can raise taxes or curtail services, neither very popular with the electorate. But if you consider that you have 7-15 percent of your revenue uncollected or 7-15 percent of your

Copyright © 2016 International Institute for Analytics

expenditures misspent, you find that you can reduce budget gaps by attacking fraud, waste, and abuse. The math is compelling. We typically see 10:1 to 100:1 returns on investment made in fraud detection and prevention. So even though budget and upfront investment can present challenges, when the investments are made, they tend to pay off on a large scale. Government leaders have to recognize the size of this opportunity to improve their financial picture and performance.

Gathering the Data

The first problem government agencies face in combating fraud is accessing the information that can help them detect or prevent improper payments. The government has an enormous amount of information about the beneficiaries in government programs like Medicare, and about the providers of services to those programs. But it struggles with accessing and leveraging all of the available information to help determine which entities are behaving appropriately within those programs, and which entities may be misbehaving, committing fraud, or abusing the programs.

In government, as in large and diverse corporations, accessing data across organizational silos often proves problematic. Some inter-agency data sharing goes on, but it tends to be very piecemeal, based on a lot of individual agreements between specific agencies to share certain kinds of data. Accessing all the relevant data is complicated by the fact that each agency and each program has its own computer systems and databases. However, that's less of a technological challenge than it used to be. Technology has evolved to a point now where we know how to combine data from multiple different sources.

There are also regulatory barriers to sharing data across agency boundaries. But just as technology has evolved, so has the regulatory landscape. We absolutely need to protect the privacy and integrity of personal information, but at the same time government should be using all available information to protect the fiscal integrity of government programs and provide the most effective services.

The final challenge, and the one that seems most difficult to quickly remedy, is culture. Government agencies are just not used to cooperating in this manner and sharing data on a large scale with other agencies. That's why our recommended approach to change is always iterative. Start small, get a core set of data and agencies working cooperatively and showing value, and grow from there. Adoption grows organically within the organization as opposed to being mandated across the entirety of government. We see more success by allowing people to move to new methods and technology at a measured pace.

Finding the Patterns

Once government agencies can bring the relevant data together, they can develop more complete views of the individuals, providers and businesses that are participating in various programs. The more information we can have about the entities, the better we can do at determining how we should expect them to behave. Then we can evaluate actual behaviors against the norm to see whether there is something aberrant going on that warrants a closer inspection. We want to determine what is normal for a certain peer group and then look for people who belong to that peer group who do not behave as their peers are behaving. We want to ask, "Based on everything else we know about this entity and its peers, is this how we would expect them to behave?"

Let's take a specific scenario. Medicaid fraud is regularly committed by "claims mills." People open a business; find a way to get a medical provider ID number, and do nothing but bill claims to the government. They don't provide any health care

Copyright © 2016 International Institute for Analytics

services; they just file fraudulent claims. Some are backed by offshore organized crime organizations. Their methods can be very sophisticated, and they know what normal claims billing behavior looks like. If we just look at their billing behavior, they look like any other large or midsize provider.

How can we distinguish the claims mills from the legitimate providers? We can look at the other ways that a provider interacts with government, and collect some information to put their behavior in context. Legitimate businesses are submitting wage and hour reporting to the government and filing tax returns. Claims mills do not have a lot of employees, and may be falsifying or skipping those reporting and tax requirements. If we can pull the information together, we get a more complete and suspicious picture: “This provider has only three employees and one licensed physician, and it only reported $100,000 in revenue on its tax returns. But its claims billing behavior makes it look like a rather large health care organization.” Even if we can’t pull all the data together, we can start with basic flags, perhaps as simple as “Did they even file a tax return?”

Leveraging Analytics

Once you start to pull all the relevant contextual data together, it quickly becomes impossible for a human to manually sift through all that information. So we need to use technology to automate the analysis of the data, find the needles in the haystack, and point them out to the people who would investigate them.

Traditionally in government, most of the analysis around fraud, waste, and abuse uses basic business rules that are looking for known fraud schemes, plus perhaps some basic outlier detection. Those methods are useful, but they cannot effectively address the more sophisticated types of fraud schemes that we see today. With business rules, you have to know about the scheme before you can write the rule. You have to be a victim first, and then you can put in a mitigating control. We need anomaly detection to notice things when we are not necessarily aware of the scheme. We are looking for behaviors that are unusual compared to what we would expect. However, anomaly detection and business rules are fairly easy for sophisticated fraudsters to get around.

We need more advanced analytics starting with predictive modeling. It looks not only at historical data about fraud, but also at the variables and conditions that are highly correlated to cases of fraud. We can see the patterns or interrelationships among various data elements that together can predictively identify instances of fraud, waste, and abuse. Predictive modeling has been a game changer in the financial services industry, and is beginning to be so in government as well.

Predictive capabilities enable government agencies to move more into prevention mode versus pay-and-chase or detect-and-recover mode. Any time we detect fraud, waste, or abuse after the fact, investigation and recovery can be very labor-intensive. And recovery may be uncertain if people disappear or are simply unable to repay. But if we can anticipate the likelihood of fraud before the payments are made, we are able to avoid all those downstream risks and costs associated with recovery.

Tax agency is one area where prevention has taken center stage. Due to the increase in identity theft and the filing of false tax returns using those identities, tax agencies now must identify fraud as it’s happening in order to prevent the fraudulent payment from going out. Unlike other types of tax evasion, with identity theft there’s little to no hope of recovering the funds since the perpetrator is hiding behind someone else’s identity. To emphasize the size and scale of the issue, the IRS was able to prevent $20 billion in fraudulent payments in 2012 by analyzing returns for identity theft prior to issuing refunds.

Copyright © 2016 International Institute for Analytics

There are also occasions to use additional advanced techniques like link analysis or social network analysis, where we are looking not just at individual entities such as participants and providers, but across the relationships among those entities. That can expose organized fraud rings or collusive activities that would fly under the radar if we were just looking at a single entity at a time. As a simple example, if we identify a tax preparer behind an unusual number of suspect returns, then the preparer is suspect and all associated returns might bear greater scrutiny. Or there could be collusion where a doctor frequently prescribes electronic wheelchairs for patients, and all of those wheelchair orders are being filled by the same durable medical equipment supplier. So looking at the connections and the relationships can help us identify risks at a network or fraud-ring level.

Prioritizing Work and Empowering Staff

Government agencies regularly work under staffing constraints. A basic way to improve fraud detection and prevention is using technology to automate traditionally manual processes. It is very cumbersome for an individual to sift through large volumes of data using manual tools. But when we can automate the processes of pulling the data out of the various sources, combining it meaningfully, analyzing the data, and drawing preliminary conclusions, investigative staff can spend less time dealing with the data and more time taking action based on it.

Analytics can also help them prioritize what work to do. It may take about the same amount of time to investigate a $10,000 tax evasion case as it does a $1 million tax case. When we can prioritize cases based on dollar value and probability of fraud, then investigators can focus on those large and important cases first, optimizing their effort and maximizing the return.

Fraud detection technology should also be able to run within the context of the underlying payment system in order to identify high risk payments before those payments are actually made. In most cases in government, you have a period of time between when a claim gets submitted and payment is made. For example, health care claims typically take 10 to 30 days to process before payment is made. So there can be ample time to analyze the claims and flag suspicious ones for review before the actual money gets paid – if there's compatibility and no time lag between claims processing and fraud detection systems.

Critical Success Factors

What does it take to succeed in implementing and then capitalizing on fraud detection technology? Here are four success factors.

- **Executive Sponsorship.** You have to start here. Senior leadership in government has to acknowledge the fact that they can do a much better job detecting and preventing fraud, waste, and abuse in government programs. The commitment to improve has got to be driven down through their organizations, because many government employees are heads down and overwhelmed with work these days, just trying to do the best job they can. So they need the directives and support coming from the top to motivate working differently. Senior leadership also has to exercise their flexibility to allocate funds and make investments in order to reduce fraud and save money.

- **Enterprise Perspective.** Governments should take an enterprise perspective on fraud prevention programs and the technology behind them. It makes little sense for each agency and program to install a different fraud detection system. That's not efficient in terms of total cost of ownership. More importantly, by taking an

Copyright © 2016 International Institute for Analytics

enterprise approach and using compatible technology, you'll find it easier to get access to that broad set of data needed for fraud detection, and you'll be able to better coordinate activities across government program areas where a single entity may be exploiting multiple programs.

- **Iterative Approach.** Rather than trying to solve big problems all at once with a huge system implementation, find an exposure area that you feel is going to have high value if you make some improvements. Start there, prove that the methods and technology work, show the results, and get further buy-in to expand. If you can deliver results within three to six months and demonstrate a very significant return on investment, momentum builds fast.

- **Workflow Integration.** Fraud detection applications and analytics should become core parts of business processes and people's workflows, not just a piece of optional technology off to the side. Successful implementation will involve business change, and it's best to identify the changes up front and work with the users, especially the fraud investigators, to understand how the technology will affect their jobs and improve their work. The goal, after all, isn't about installing technology. It's about dramatically improving operational and financial performance by detecting and preventing fraud in government programs.

Additional Information

To learn more about this topic, please visit www.sas.com/security.

Copyright © 2016 International Institute for Analytics

About the Authors

Greg Henderson

Greg Henderson is the Head of the Security Intelligence Global Practice at SAS. He is responsible for developing and supporting SAS' global strategy related to fraud and security solutions including developing the overall go-to-market strategies, business development strategies and pre-sales and post-sales solution support.

Greg has over 15 years of experience in fraud and security in both the public and private sector, and has been on the forefront of SAS' solutions for banking fraud, anti-money laundering and terrorist financing, and most recently in developing SAS' enterprise approach to fraud and security risk detection and prevention in the public sector.

Greg is a published author of several papers, is a frequent speaker at industry conferences and has provided legislative testimony on the topic of fraud and security on several occasions. He holds a Bachelor of Science degree from Bowling Green State University, and resides in Raleigh, NC.

Robert Morison

Robert Morison serves as Lead Faculty for IIA's Enterprise Research Subscription. An accomplished business researcher, writer, discussion leader, and management consultant, he has been leading breakthrough research at the intersection of business, technology, and human asset management for more than 20 years. He is co-author of *Analytics At Work: Smarter Decisions, Better Results* (Harvard Business Press, 2010), *Workforce Crisis: How to Beat the Coming Shortage of Skills And Talent* (Harvard Business Press, 2006), and three Harvard Business Review articles, one of which received a McKinsey Award as best article of 2004. He holds an A.B. from Dartmouth College and an M.A. from Boston University.

iianalytics.com

Copyright © 2016 International Institute for Analytics. Proprietary to subscribers. IIA research is intended for IIA members only and should not be distributed without permission from IIA. All inquiries should be directed to membership@iianalytics.com.

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies.
107974_G37290.0916