INTERNATIONAL INSTITUTE FOR ANALYTICS™

CLIENT ONLY

DISCUSSION SUMMARY
RESEARCH & ADVISORY NETWORK

Reducing Fraud in Government Services: Analytics to Find and Fight the Fraudsters

STEVE BENNETT
Director, Global Government Practice, SAS

JON LEMON
Solutions Specialist, SAS Federal

NOVEMBER 2016

Discussion Overview

Improper payments and other forms of fraud cost government agencies and taxpayers $300 million a day. Agencies struggle to make headway against fraudsters who are both inventive and technologically well-equipped. But progress is possible through the combination of data management and integration, advanced and embedded analytics, and information and insights channeled to decision-makers. To explore the challenges of fighting government fraud and the opportunities to reduce losses, IIA spoke with Steve Bennett, Director, Global Government Practice at SAS and Jon Lemon, Solutions Specialist, SAS Federal.

Please describe the landscape of government fraud. What are the challenges, and how has the landscape changed in recent years?

Steve Bennett (SB): Fraud and improper payments remain a significant challenge for governments at all levels around the world. Any agency that engages citizens for the provision of benefits or for collecting or disbursing of funds finds itself at risk. In 2014 alone, the U.S. Government Accounting Office estimated that federal agencies lost about $125 billion in improper payments. Despite a lot of hard work and good progress by government officials in recent years, that number continues to rise. So this is a very big problem. Given that we're in an era of flat or shrinking government budgets, plus the pressure for more efficient delivery of services to citizens, I would say there has never been a more urgent need to combat fraud and improper payments and reduce loss to the taxpayer.

It helps to think about the landscape in terms of two different types of crimes. One is information-based assaults and threats, including intrusion, cybersecurity attacks, insider threats, fraudulent benefits claims, and other improper payments. In the other, fraudulent activity is used to commit more physically based crimes, including immigration violations or even terrorism.

Jon Lemon (JL): What's new in the landscape is the sheer volume of data generated and the technologies for working with it. Decades ago there might have been just a couple of data sources from which the government — and the criminals — could work. Now the data is growing exponentially every year, coming in automatically from systems and sensors in the field and from citizens themselves. That's a good thing and a bad thing. It provides us a lot more opportunity for us to fight the criminals, but it also gives the criminals a lot more opportunity to find cracks in the data, the security set up to protect it, or the agency work processes using the data.

Compounding the problem is the difficulty of sharing data across agencies and jurisdictions. Privacy concerns prevent data sharing. For example, in the FBI name check system, applicants for gun purchases cannot be shared with the ATF for investigative profiling purposes, just as FBI data that has anything about U.S. persons cannot be shared with the CIA, NSA, or many other Intelligence Agencies. There are policies that keep data siloed, but some initiatives are underway now to reduce those barriers in a well-thought-out manner.

What are the roles of analytics in finding and reducing fraud?

JL: Government agencies need to employ a variety of analytical techniques in fighting fraud. The most common one today is business rules, which are basically if/then statements: "If the transaction is over $10,000, send it to review; if it's under $10,000, then process it." But rules have a lot of vulnerabilities. It's easy to find out what they are. A fraudster will test the system with transactions at $7,000, then $9,000, then have one rejected at $11,000 and have a good idea where the cutoff is. Rules are great at catching inadvertent errors, like when someone miskeys and adds an extra zero in an amount. But they look at transactions in isolation and so they can't detect patterns like the fraudster stair-stepping amounts. They have their place, but they're not the strongest defense.

You need anomaly-detection techniques in order to look across transactions and find the patterns. One approach is to develop profiles of what bad guys look like and the patterns in their behavior. Then cast the transaction in question against those profiles and see if it matches that of a bad guy. If the transaction has a certain frequency, or is done on a certain time of day, or is for a certain dollar amount, or whatever it is, you can look at it and say, "We've seen this pattern before, and this looks suspicious, so we'd better investigate."

Another approach is to compare the transaction to its peers by transaction type or size or any other important characteristics. When you can look at a large population, you can determine what transactions are within a standard range in all respects, and thus present a low risk of fraud. But a transaction several standard deviations outside the norm would generate a higher risk score and earn some scrutiny.

Link analysis is a third technique that's being used more frequently these days. If we're able to link the different entities and players — for example, Medicare patients and their conditions and their medical providers — we can test entire networks for anomalies or model their behaviors. That makes it easier to see if the network itself or any of its key players, such as the medical practice systematically overcharging Medicare, is cause for concern. Often the fraudulent individual can fly under the radar screen, but the network as a whole cannot.

SB: I'll just add that these analytical efforts really need to be focused. Think about the volume and variety and complexity of the data that government agencies have to deal with. Analytics has become an important mechanism for helping make sense of all that data. But too often, people rush off and start to talk about techniques without clarity around business objectives and the roles that analytics can play in meeting them. I use as my touchstone the definition of analytics from INFORMS, the largest professional society for analytics. They define analytics as the scientific process of transforming data into insight for making better decisions. So you've got to ask what data you have and need, where you need greater clarity or specific insight, and what specific decisions you're trying to make and improve upon. And how can you improve decision-making not just at the transaction level, but improve the decision-making process at the highest levels in an agency or government office?

What challenges do you see most often when using analytics to fight fraud?

JL: Each of those three pieces — organizing data, transforming data into insight, then embedding the insights into how people and processes work and make decisions — present challenges. But for most government agencies, data management remains the

biggest. Analytics need good data, not perfect data but data sufficient to the objective at hand. Many agencies today still manage data in spreadsheets and files spread across systems and employees' workstations and laptops. It's no wonder we may not always be able to tell if the same person is receiving three benefits payments if their name is spelled differently in three different versions of a file. Some agencies might still be relying on voluminous paper records. If you've heard stories about government records retired in caves buried in the hills in western Pennsylvania, they're true. It takes months to get certain things processed because the records have to be looked up on paper in a cave.

Once you have data in electronic format, it is still going to be noisy, messy, full of inconsistencies and duplication. And sometimes the most potentially useful data is of multiple types, both structured in databases and unstructured such as text. Data management is the foundational challenge.

SB: We of course don't want to be paper-bound, and having electronic data and automated processes create necessary efficiencies. But they also create openings for the bad guys. I said "necessary" efficiencies because agencies are under pressure to get benefits to citizens without bureaucratic delay. There are deadlines built into legislation saying benefits must be provided within X days of the citizen's application. To speed things up, processes must be electronic and automated, often with little or no human review of transactions and decisions. That plays into the hands of criminals who can exploit weaknesses in how automated evaluations and decisions are made.

Government is ultimately more concerned with getting benefits to the right people than with preventing money from falling into the wrong hands. And they get things right the overwhelming majority of the time. With the Food Stamp Program, something like 98 percent or 99 percent of the money helps low-income families with food purchases. However, they still have a 1 percent or 2 percent fraud problem, which adds up to over a billion dollars a year. Individual acts of fraud aren't going to have a big effect, but many events in the aggregate add up to significant loss. We're focusing here on fraud prevention, but government agencies also need advanced analytics to automate processes and decisions in the first place — in as accurate, efficient, and airtight a way as possible.

Most discussion of government fraud seems to focus on the information-based assaults. What about the physically based crimes?

SB: With information-based crimes, we typically have a large population of events to examine for patterns. And as I just mentioned, each event has rather limited consequences. With more physically based crime, let's say immigration fraud, we have a smaller population of events, single events can have larger consequences (for example, if the illegal entrant is a terrorist), and we often don't have the benefit of time to look statistically for large, complex patterns. The operational decision might have to be made at a border or an airport in near real time, and the analytics challenges in the information that you might have to draw from are very different. The answer is less often a clear and automated yes or no. The best result may be "We should pull this guy aside and ask him a few more questions."

JL: The challenge is similar to detecting credit card fraud, though the available information may be much less and much more uneven. The bank has to scan large amounts of available data and score each transaction for likelihood of fraud in a split second. It compares each new transaction with profiles of good and bad transactions, with special attention when expected information is missing. With both physical

and information-based fraud, governments are never going to completely stymie the criminals. As soon as we set up a barrier, they're at work devising ways around it, so we need to spot each new fraudulent technique as quickly as possible. The goal is to mitigate the effects of as many of those smaller events as possible, but especially to anticipate and prevent the few more catastrophic events.

What are the differences between government and commercial organizations in addressing the challenges we've discussed?

JL: Despite all efforts to be more efficient and speed up cycle times, government agencies are still more bureaucratic than commercial organizations. We tend to think of bureaucracy as a bad thing, but it has some advantages in terms of checks and balances and accommodating a lot of stakeholders. But bureaucracy does slow things down, especially when it comes to government budget and bidding and procurement cycles. It takes much longer to get new capabilities, including new analytics, in place. And that's a big disadvantage when trying to keep pace with the inventiveness of the bad guys.

Another disadvantage was mentioned earlier — by design, government agencies aren't allowed to assemble all the data that might help in fighting fraud. Some industries like health care also have obligations to protect the privacy of individuals, but for the most part, commercial enterprises have a lot more freedom to assemble and analyze their data.

SB: In the commercial sector, decision-making is usually fairly centralized, even in public companies where executives have accountability to shareholders and a board of directors.

Given the pressure to stay ahead of the competition, decision-making is usually fairly rapid as well. Government is pretty much the opposite. Decision-making is diluted and distributed instead of concentrated and centralized. Some of that is by design, going back to how the Constitution structures the government. The founding fathers wanted to prevent too much concentration of power and to discourage precipitous action. But today, governments must adjust to a fast-paced world of electronic communication, big data and analytics, and often activist citizenry.

Given their profit motive, commercial businesses may be less tolerant than government of losing money to fraud in pursuit of customer service, especially if customer service is already fast and efficient. The government simply is not directly accountable to taxpayers in the same ways businesses are to shareholders.

How would you summarize the success factors in fighting government fraud?

SB: Useful data, a variety of basic and advanced analytics, a versatile technology platform to support the data and analytics, and a receptive organization — those are the fundamental success factors. The organizational piece involves both operational changes to how people work and cultural changes to how they deal with information. Are people curious enough to look at things in new ways, experiment a bit, and develop new insights? Are they ambitious enough to capitalize on analytics and move way beyond business as usual?

JL: Behind the scenes, skill sets are a critical success factor that is especially challenging for government agencies. Organizing and integrating vast amounts of data, experimenting with and selecting the best algorithms for analyzing the data, building models and

then operationalizing the analytical outputs in people's workflows, designing and managing the technical architecture — those are all advanced skills. People with them tend to gravitate toward commercial enterprises where pay scales are higher and pace is faster than in government agencies. Today there's intense competition for cybersecurity experts across commercial sectors, when the need for those skills may be greatest in government. All that points to why government agencies need to be more flexible with pay and working arrangements, more agile in their technology development methods, and smart about sourcing and partnering with outside expertise.

What does the future hold in terms of both threats and the analytics to combat them?

SB: The threats will continue to proliferate and become more sophisticated because the same analytics tools that agencies have are available, often in open source, to the fraudsters and criminals. And they can often put the tools to work faster. An old Navy pilot friend likes to talk about the OODA loop — observe, orient, decide, and act. The pilot who can do that faster wins the dogfight. When government moves slowly, the bad guys can win more often.

That said, some of the techniques that are being developed in artificial intelligence and machine learning are going to be of immense value in recognizing the bad guys and preventing improper payments before they go out. If, instead of having to know upfront exactly what to look for, the systems can learn what to look for on the fly and find the attributes predictive of fraud, the good guys might gain the advantage of an extremely fast response. Another technology area with immense potential is cloud computing. Taking analytics off-premise into secure clouds can make agencies much more nimble in putting analytics to work in intercepting fraud. If the technology environment is at the ready, the agency has a way to mitigate the mission impacts of the long and tedious government procurement cycle.

If agencies want to turn the corner in fraud prevention, they have to exploit the one big advantage they have — their data. No fraudster can gather all the data potentially available. Only the government has the ability – should it decide to do so – to consistently link DMV data with Social Security data with Medicare data. The bad guys have to act more locally. If agencies can look across more data, they can better detect the local anomalies. But we're back again to the governmental restrictions on data sharing, and citizen concerns about possible misuse of their private data.

JL: As an example of the importance of data sharing, the government has been trying to address the challenge specifically for Homeland Security. Some 70 "fusion centers" across the country promote sharing of FBI, CIA, Justice Department, military, and state and local government data. Their effectiveness has been called into question, but the need and opportunity are real. An enormous amount of data is generated by sensors as well as conventional systems — dashboard and ATM and security cameras, automated highway toll system data, credit card transaction data. Fusing it together enables rapid response, as with the recent bombings in New York and New Jersey. Or better yet, anticipation and prevention of terrorist acts. Internet of Things data will play bigger and bigger roles in preventing physical crimes. We need to clarify privacy expectations and surveillance limits in light of all the data we're generating.

To wrap up, what are the top things government leaders and technologists should know and do around analytics to find the bad guys and prevent fraud?

JL: First, approach analytics for fraud prevention as a complete end-to-end process. Generate and assemble data, apply analytics, get information and insights into the hands of decision-makers, and embed analytical decisions in automated systems. Keep in mind that adopting better analytics will have a limited effect if you're not working on all the components and how they work together.

Second, for operational analytics and embedded decisions, anticipate how fast you are going to scale up. There's an enormous difference between models developed in the lab and systems scanning billions of records a day and delivering results with sub second response time.

Third, get going. The data management and other challenges may be great, but you've got to start somewhere in advancing analytical capabilities to keep pace with the threats. Don't delay trying to devise the 100 percent solution because there's no such thing. This effort never stops, and the best solution is to be agile and adaptable.

SB: I have four recommendations for government agency leaders:

- **Be an integrator.** Gather and arrange the information that you already have. As Jon suggested, start wherever you are. Once integrated, the data that most agencies and government offices have is sufficient for developing better analytics to prevent fraud and improve stewardship of taxpayer resources.
- **Be curious.** Seek new data sources that may be directly or indirectly related to your decision space. Look for creative ways to find and apply data and discover its predictive power. Social media data, for example, is used in all kinds of novel ways that people didn't think about beforehand.
- **Be open.** Accept that conventional wisdom might be challenged as evidence and analytical insights emerge. Some people are all in favor of data and analytics until the insights they produce suggest doing things differently. You've got to use data and analytics as levers for change.
- **Be patient.** Even when you're open to it, change takes time. Organizational and cultural change require at least as much time and energy as technological change. Leaders can accelerate adoption of analytics solutions for better decision-making, but driving change requires a bit more patience in government than in the commercial space.

Additional Information

To learn more about this topic, please visit http://www.sas.com/fraudresources

About the Interviewees

STEVE BENNETT

Steve Bennett drives strategic industry positioning and messaging in global Government markets. A thought leader in decision science and the application of analytics in Government, Steve works to enable delivery of effective solutions to Government customers around the world.

Prior to SAS, Steve held a number of leadership positions during his 12 years in the U.S. Department of Homeland Security. Following the events of September 11th 2001, Steve led the design and application of quantitative analysis to inform some of the United States' most challenging security decisions, most recently as the Director of the National Biosurveillance Integration Center. Over the course of his career in Government, he led diverse teams to provide analytic decision support to senior officials in the White House and across the U.S. Government Executive Branch. Steve has a passion for improving Government decision making, and pursues better organization, management, and understanding of Government data as critical to that endeavor.

Steve holds a doctorate in Computational Biochemistry from Stanford, as well as undergraduate degrees in Biology and Chemistry from Caltech, and has authored a number of peer-reviewed and other publications. When not supporting improved analytics in Government, he is coaching youth soccer, leading children's ministry at church, or building something in his workshop.

JON LEMON

Since joining SAS in August of 2007, Jon's primary focus has been working with Federal, State, and Local Government customers to understand organizational effectiveness and their performance against stated objectives. He leverages his past experience to help customers implement industry leading performance management, workforce analytics, costing, and fraud prevention solutions through the integration of technology, processes, people, and methodologies.

Prior to joining SAS, Jon was a Budget Director at the Department of Homeland Security where he formulated, executed, and managed over $4.5 billion of appropriated funds annually. Jon also worked with Booz Allen Hamilton where he honed his skills in performance management and fraud detection and prevention while supporting various Chief Financial and Program Management Offices throughout multiple federal civilian and defense agencies. He earned his MBA degree from the Florida Institute of Technology and also holds a Finance Bachelor of Science degree from the University of North Carolina at Wilmington.

IIANALYTICS.COM