The State of Fraud In Government

Many agencies highly regard their ability to use data analysis to combat fraud, abuse and improper payments, but TechWeb's research shows there is room for improvement.

An Exclusive TechWeb Research Survey

By David Stodder

An exclusive TechWeb survey of 327 federal, state and local government decision-makers examined the state of fraud. Many agencies regard their ability to use data analysis to combat fraud, abuse and improper payments as good or excellent, but TechWeb's research shows that most organizations are not fully mature in the use of analytics. This report explores key directional trends in using business analytics to combat fraud.

Sponsored by

sas

Few organizations, much less individuals, are untouched by the problem of fraud and improper payments. Nearly every day in the news, there are stories such as one reported recently in *The New York Times* of a crime syndicate charged with Medicare fraud. A network of suspects reportedly "stole the identities of doctors and thousands of patients, using them at more than 100 bogus health clinics in 25 states to bill Medicare for more than $100 billion." According to CBS News, Medicare fraud alone totals $60 billion a year. Cybercrime costs individuals at least $7 billion, and other forms of fraud cost additional billions. Fraudulent workers' compensation claims are driving insurance rates so high that in some states, companies are being forced out of business.

Public and private organizations employ tools and applications for data analysis and predictive analytics to battle both the rising incidence of fraud and improper payments and the increasing cost of detecting and preventing them. Data analysis steps include preparing and modeling data to support different types of analyses as well as business intelligence reporting, querying, visualization and aggregation, so that decision-makers can make fact-based decisions. Predictive analytics are driven by advances in the use of data mining tools and techniques to provide insight into trends, patterns and events that could impact the future. Among organizations using these tools and applications today are federal, state and local governments. As enforcers, regulatory watchdogs and investigators, governmental agencies are on the front lines, and as potential targets of fraud, they are challenged to detect and prevent incidents against themselves.

While more than half of federal, state and local government organizations surveyed by TechWeb regard their current ability to use data analysis to combat fraud, abuse and improper payments as either good or excellent, the research found that most organizations are not yet fully mature in their use of the technology. Many are still focused primarily on identifying the right data sources and enabling access to them, rather than engaging in more advanced steps such as predictive modeling and analysis. About half say that a lack of resources and budget hinder their ability to establish a business case for deploying data analysis methods, tools, applications and services to combat fraud.

:: Goals and Objectives in Combating Fraud

With resources and budgets under pressure, it's not surprising that the largest percentage (68%) of survey participants cite reducing the cost of combating fraud, abuse and improper payments as an important benefit they seek from implementing data analysis and predictive analytics *(see Figure 1)*. Tools and applications for data analysis can help organizations bring down costs by introducing automation to replace costly and often routine, time-consuming manual steps. One area where data analysis efforts can bog down is in the basic steps for data collection and reporting — steps that tools can improve, especially as data sources get bigger and the time interval within which users need to see the analysis gets smaller, even approaching real time. Nearly one third of survey participants regard data collection and reporting steps as a pain point, with other data management tasks also prominent *(see Figure 2)*.

Many organizations want to detect and prevent fraud with the end goal of increasing the efficiency and effectiveness of payment processes. Improving auditor and investigator

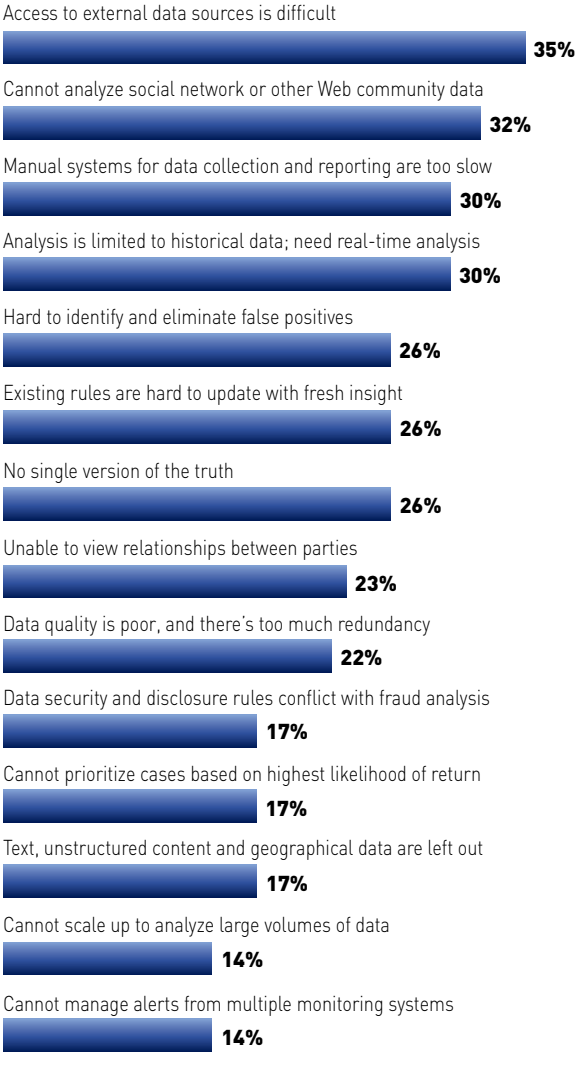
Figure 1. How important is each of the following benefits to your investment in data analysis methods, tools, applications and services to combat fraud, abuse and improper payments?

Source: TechWeb Research. 322 respondents working in Federal, state or local government or consulting with government.

Methodology:

In October 2010, TechWeb conducted a study on behalf of SAS on the State of Fraud in Government. The survey was conducted online via our survey host partner, SurveyGizmo. Invitations were emailed to TechWeb's qualified database of technology decision-makers. A total of 327 respondents qualified as working in government (Federal, state or local or government consultant). The survey has a margin of error of 5.4 percentage points.

Figure 2. Which of the following information management and technology "pain points" do you encounter in performing data analysis to detect, analyze and support decisions to combat fraud, abuse and improper payments?



Source: TechWeb Research. 286 respondents working in Federal, state or local government or consulting with government.

efficiency and ROI is a goal of 61% of participants. More than half (58%) of federal government participants regard reducing improper payments and setting more accurate target loss rates as an important benefit of fraud data analysis; 60% of state and local government participants share this objective. Overall, 59% of organizations want to increase payment integrity without harming process performance. Analytics can help organizations separate valid and invalid healthcare claims, for example, so that valid claims are processed quickly and invalid ones are spotted before they infect downstream processes and result in costly billing and payment errors. Catching fraudulent activity before payments are made can save government organizations millions of dollars annually.

TechWeb asked what types of fraud, abuse or improper payments survey participants are targeting with current or planned deployment of data analysis methods, tools, applications and services. Somewhat surprisingly, employee fraud was the most common answer (54%). A sensitive issue, employee fraud has quietly become a significant problem for public and private organizations of all sizes. According to a study by the Association of Certified Fraud Examiners, U.S. organizations lose 7% of their annual revenues to employee or occupational fraud schemes, which the Association says can go on for years before being detected.

In the TechWeb survey, however, most participants who selected employee fraud also indicated several other types of fraud (participants could check all that applied). A state government CIO participant, for example, targets 16 different types of fraud for his organization's data analysis. The superintendent of a state capitol targets seven types. Prominent targets indicated by participants include computer crime including cyber-theft, billing fraud, asset misappropriation and government fraud and corruption. Workers' compensation fraud and worker misclassification were selected by 21% and 13%, respectively. Healthcare fraud, with targets spread across billing (43%), benefit (17%), insurance (12%), Medicare/Medicaid (9%) and healthcare product fraud (8%), added up to a significant focus at both federal and state/local levels.

:: What Government Organizations Do and Plan to Do

The most prevalent fraud detection and prevention focus at both federal and state/local government levels is on analyzing financial information and relationships. The most common steps are to audit financial statements, billing and contracts (68%). Such analysis is important to investigating adherence to generally accepted accounting principles (GAAP) and for improving transparency and accountability inside government organizations and in industries monitored by government bodies. Half of survey participants are investigating financial relationships for conflicts of interest, and 39% are flagging high-risk transactions and payments for extra review. To carry out these steps, 58% have already established an audit or investigative department and another 10% plan to do so.

Many organizations are formalizing their policies and programs, which is essential for maintaining consistency across organizations and providing direction and context

for data analysis. Nearly three out of five organizations already develop and manage written fraud policies, and half have already adopted compliance and integrity programs; another 15% plan to do so.

The research shows that case or claims management systems are the most common type of software applications used by government organizations in the fight against fraud. However, these applications are designed primarily for managing case or claims management processes, not fraud data analysis. Most organizations therefore need specialized tools and applications for data management and analysis, especially as the challenges become bigger and more complex. TechWeb found that the majority of organizations have yet to deploy data management and analysis for detecting fraud, abuse and improper payments. Just over a third (35%) of organizations currently uses data warehouse systems and appliances, with less than a quarter implementing BI, OLAP or more advanced data analysis tools. *(See Figure 3.)*

TechWeb asked participants to characterize whether their approach to detecting, analyzing and taking steps to combat fraud is proactive, active or reactive. The answers offer insight into the maturity of organizations as they apply data analysis. The highest percentage (43%) regards themselves as active; they monitor transactions, payments and other data but have limited capabilities for predictive modeling and scoring. The next largest group says they are only reactive (29%); they are limited to responding to fraud on a case-by-case basis, and can only analyze incidents and behavior after the fact. The survey found that a larger percentage of state and local governments are reactive compared to federal government organizations (35% to 21%, respectively). Trailing the majority are "very reactive" organizations that do little monitoring for fraud and are struggling to comply with regulations and internal policies (9% overall).

:: Predictive Analytics for Proactive Organizations

At the leading edge are proactive organizations that employ predictive analytics to model and score fraud risks, uncover patterns and anticipate damaging incidents or behavior. Overall, 19% of participants say their organizations are proactive; 27% of those from federal government organizations describe themselves as proactive compared to just 12% of those from state and local government.

Proactive organizations use predictive modeling and analytics to examine data for relationships between current and predictive variables, which can point to complex sets of claims that are fraudulent. An example would be "unbundled" sets of claims submitted by healthcare providers that have used different codes to refer to the same procedure. Predictive analytics exploit computing power to spot patterns particularly in large data sets that would either not be apparent to human investigators or would take much longer to uncover. In most cases, predictive analytics tools and methods do not replace data analysts but are instead used by them. Predictive modeling that is flexible and can be updated to reflect the ever-changing tactics of fraudsters brings an additional level of fraud detection to the forefront.

Figure 3. To combat fraud, abuse and improper payments, is your organization currently using, or planning to use in the near future any of the following methods, tools, applications or services?

	Already deployed	Within one year	Within two years	No plans
Case or claims management	41%	6%	3%	14%
Business rules management	36%	9%	6%	13%
Data warehouse/data appliance	35%	9%	5%	15%
Alert management/Activity monitoring	35%	6%	2%	18%
Fraud detection and alert generation	34%	9%	6%	12%
Event processing and analysis	33%	7%	3%	16%
Identity resolution	26%	10%	6%	15%
Data quality, matching or profiling	26%	10%	6%	15%
Business intelligence/OLAP	23%	11%	4%	18%
Predictive modeling, analytics and data mining	18%	8%	7%	20%
Text or geospatial analytics	17%	7%	5%	23%
Social network and/or link analysis	15%	9%	5%	26%
Hosted or software-as-a-service data analysis	13%	8%	5%	26%

Source: TechWeb Research. 317 respondents working in Federal, state or local government or consulting with government.

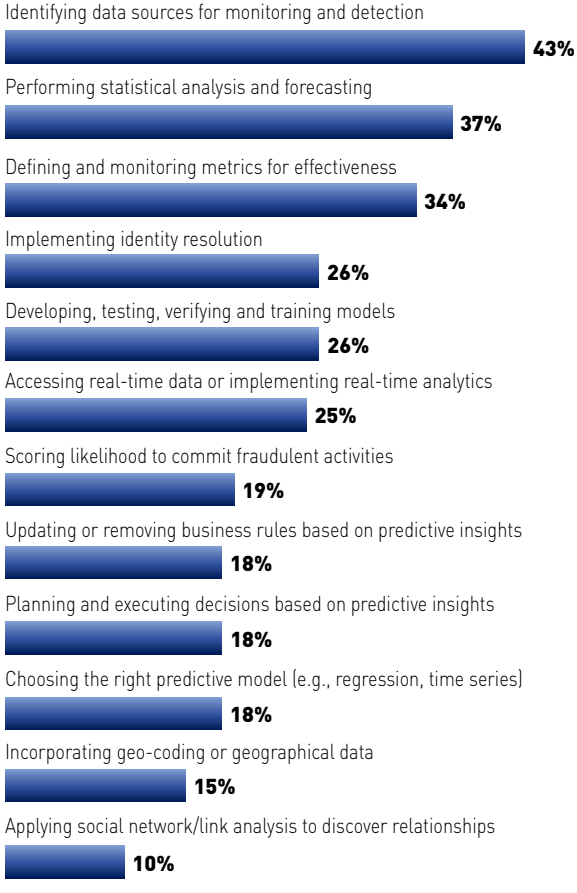
More than half (56%) of participants say that predicting the likelihood of fraudulent events or behavior is a benefit they seek from their investment in data analysis. However, only 23% currently employ data mining and predictive analytics, and just 28% analyze, model and score potential risks and threats. Some of the frustration behind this sort of discrepancy between desired benefit and actual steps taken is found in the answers supplied by a state comptroller participant focused on healthcare and Medicaid fraud. He says that while his organization finds it important to predict the likelihood of fraudulent events, it has no plans to employ data mining and predictive analytics and only within two years plans to score potential risks and threats. Lack of resources and executive support are stumbling blocks.

The survey found that only 10% of organizations are very satisfied with their current software and services for enabling predictive analytics and 33% are somewhat satisfied. Interestingly, only a minority of participants says their organization is using tools from recognized data mining and predictive analytics tool providers; the majority is using systems from the market-dominant BI, spreadsheet and database software providers. This suggests that organizations may currently lack the appropriate tools to accomplish more advanced data mining and predictive analytics objectives.

Beyond identifying data sources, as noted earlier, the data mining or predictive analytics steps that the largest percentage of organizations is taking are statistical analysis and forecasting (37%), followed by defining and monitoring metrics for effectiveness (34%). Just over a quarter (26%) are developing, testing, verifying and training models, which is the continuous process that characterizes most data mining and predictive analytics efforts. Less than one fifth (18%) say they are planning and executing decisions based on predictive insights, with only 8% of participants from the federal government indicating they are doing so (compared to 19% of those in state and local government). *(See Figure 4.)*

Overall, 23% are satisfied with the degree of software automation in their predictive analytics model development, comparison and testing; 22% are satisfied with automation for variable creation and selection; and 21% are satisfied with the automation of their classification, pattern matching and gap analysis steps. These results suggest that most organizations are still unsatisfied, and are in the early stages of automating data mining and predictive analytics steps; as yet, they do not rely fully on software to accomplish them.

Figure 4. Which of the following advanced data analysis, data mining or predictive analytics steps are you or those in your functional area performing as part of efforts to combat fraud, abuse and/or improper payments?



Source: TechWeb Research. 239 respondents working in Federal, state or local government or consulting with government.

:: Social Network Analysis: The Cutting Edge

As the use of online social networks expands, they have unfortunately become breeding grounds for sophisticated fraud schemes, such as phishing and skimming. Crime syndicates have been using social networks to hide their affiliations as they pursue many types of fraud beyond cyber-crime, including Medicare and Medicaid fraud. Thus, it is important for organizations to evaluate how they can incorporate social network analysis into their efforts to combat fraud, abuse and improper payments.

Survey results suggest that concern about social network use for fraud is rising. The second most common information management and technology pain point cited by participants was the inability to analyze social network or other Web community data (32%). While about one quarter (24%) of participants say that they currently monitor and analyze social networks, only 15% are using social network or link analysis methods, tools, applications or services. These results suggest that many organizations are using manual processes and have not yet implemented software.

:: Healthcare and Workers' Comp: Growing Need for Analytics

The TechWeb survey provides a closer examination of how governmental organizations are implementing analytics for fraud detection and prevention involving two complex and costly areas: healthcare and workers' compensation. Let's first look at healthcare.

The survey offered participants a choice of 15 frequently encountered fraud, abuse or improper payment instances that involve benefit, billing, healthcare product, insurance and Medicare or Medicaid fraud. The survey results show the instances for which the largest percentages are implementing data analysis and predictive analytics. The top instance is to uncover cases of billing for services not provided, not necessary or at too high a rate (34%). This is followed closely by hidden conflicts of interest, kickback or other relationships (33%). The third most-common instance drawing analytics implementation is claims irregularities, such as duplicates or too many claims to one provider (32%).

As fraud relationships exploit social networks to extend their reach, organizations may need to implement social network or link analysis tools to monitor hidden conflicts of interest behind healthcare claims. One third of participants from state and local governments are using analytics to track fraud across multiple providers, services and goods. Concealed connections between seemingly independent perpetrators who are attacking multiple healthcare entities may be easier to spot through analysis of patterns, relationships and links found in online data sources and social networks.

Workers' compensation instances that most attract implementation of data analysis and predictive analytics are, first, worker activities that are inconsistent with reported injuries; and second, overbilling by medical providers for treatments not rendered (58% and 44% respectively). While these results are the same when we look only at participants from federal government organizations, state and local government participants find analysis of discrepancies in workers' injury descriptions (61%) and discovery of employees working under the table while receiving compensation (58%) the two most important. Participants from state and local governments are also focused on using analytics to isolate high-risk, exceptional claims that slow down processes (41%). This result is in line with the earlier observation that organizations want to use analytics to find troublesome claims earlier, so that processes for good claims can run more efficiently.

:: Analytics Begin with Good Data

The TechWeb survey found that organizations have ambitious goals for using data analysis and predictive analytics to reduce costs, improve processes and anticipate next moves by those who are intent on committing fraud. Yet, in many cases they are not mature in their implementation of software to automate routine data analysis tasks and exploit computing power to examine patterns in larger data sets and address demand for more timely analysis. In other words, there is plenty of room for growth in the use of analytics by governmental organizations to both monitor behavior in industries they are responsible for regulating and to reduce fraud perpetrated against government bodies themselves.

However, analytics are only as good as the data. Organizations are still spending much of their time on enabling access to multiple data sources and preparing data for analysis. About one fifth of participants say that poor data quality and too much redundancy are pain points. Nearly a third (30%) of participants encounters frustration with having only historical data to analyze when decision-makers need real-time analysis. Thus, to reach the potential of data analysis and predictive analytics tools and methods for combating fraud, abuse and improper payments, organizations cannot overlook the need to solve data management challenges that may be the biggest stumbling blocks to more rapid progress.

About the Author:

David Stodder is an independent analyst, writer and researcher focused on innovative uses of information to achieve business and IT objectives. He heads up Perceptive Information Strategies. Stodder has provided thought leadership in information technology management for over 20 years. He was previously VP and research director at Ventana Research and the founding editor of *Intelligent Enterprise*.