Agencies Armed Against Fraud

Study finds the right technology helps government combat fraud, abuse and improper payments.

Executive Summary

The UBM Tech 2013 State of Fraud in Government survey shows that federal, state and local agencies and departments recognize the importance of using technology to combat fraud, abuse and improper payments. Yet a lack of understanding and knowledge, along with the perception of the high cost of solutions, may be holding some agencies back — at a time when the need for technological assistance in fighting fraud is at an all-time high.

The survey of 211 federal, state and local government decision makers revealed that agencies are dedicating more staff to fraud detection and prevention overall, and a healthy percentage have either purchased solutions over the past 12 months or plan to do so. Those who aren't using technology to aid in fraud prevention and detection cite cost concerns and lack of awareness of technology options as key barriers.

The results of the UBM Tech research explore key directional trends in the level of adoption of fraud detection tools among government agencies, as well as the perceptions of agencies and departments toward fraud in government.

In this paper, we highlight the results of the survey and share examples of how various agencies have been successful in fighting fraud, abuse and improper payments, and in overcoming cost barriers.

Data in government is growing at an unprecedented rate — not only structured data, but unstructured data from social media, sensors, images, audio and GPS. The velocity, variety and volume of data growth will continue unabated. These factors make fraud, abuse and improper payments more difficult to catch without the use of sophisticated technology. Today, advanced technology is the only way to make sense of all that data quickly enough for government agencies to take effective action.

By employing the right technology, agencies can more quickly and effectively detect abnormal patterns, automatically escalate suspicious cases for further investigation and determine areas and activities that are most likely to lead to fraud, abuse or improper payments.

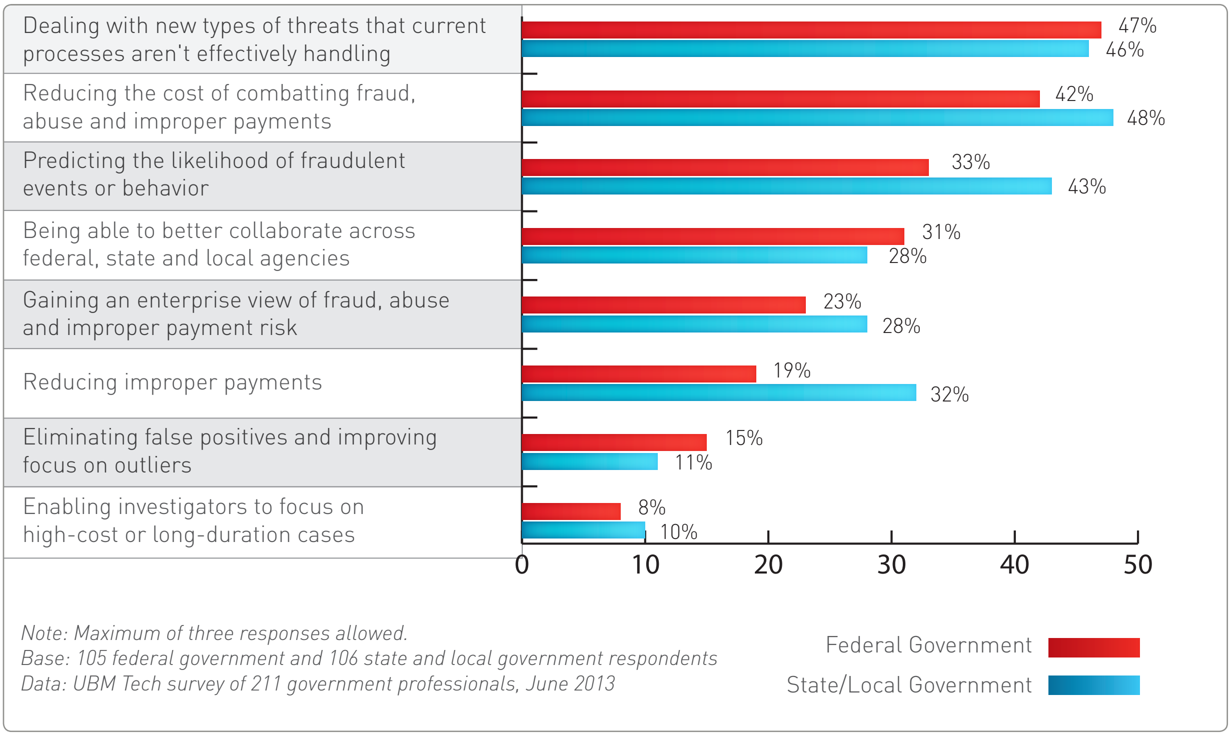
Federal, state and local survey respondents consistently cited three top drivers for using fraud detection and prevention technology: dealing with new types of threats that current processes aren't effectively handling; reducing the cost of combating fraud, abuse and improper payments; and predicting the likelihood of fraudulent events or behavior (**see Figure** 1).

Sponsored by

sas

UBM Tech

Figure 1. What are your agency's or organization's key drivers for using fraud detection and/or prevention technology or for planning to deploy the technology?



Note: Maximum of three responses allowed.
Base: 105 federal government and 106 state and local government respondents
Data: UBM Tech survey of 211 government professionals, June 2013

Government organizations across the board understand the importance of using technology to combat fraud, abuse and improper payments. Many have added staff dedicated to fraud detection and/or prevention, and a healthy percentage have either purchased solutions over the past 12 months or plan to do so.

Technology helps combat fraud, abuse and improper payments by:

- Identifying "hot spots" where fraud, abuse or improper payments may be taking place, such as the IRS, which has identified hundreds of thousands of cases of identity theft, or the Medicare system, where overpayment due to error or fraud is rampant;
- Identifying what type of fraud, waste or abuse may be taking place, such as forgery or altering of documents, theft, misappropriation of funds, identity theft, improprieties in the handling and reporting of financial transactions, the destruction of property or records, and overlapping programs that result in overspending;
- Identifying specific people or other sources that should be investigated. While the first step is identifying what type of fraud, waste or abuse is taking place, the next step is drilling down to determine who might be responsible. This can be done through predictive analytics, social network analysis, text analytics or data mining tools.

Methodology

In June 2013, UBM Tech conducted an online survey on behalf of SAS exploring the state of fraud in government.

UBM Tech collected data from 211 business technology professionals at federal, state and local government agencies through an online survey. More than 60 percent hold C-level, director or manager job titles, and nearly two-thirds are from agencies with more than 500 employees.

The greatest possible margin of error for the total respondent base (N=211) is +/- 6.7 percentage points. UBM Tech was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices.

While the obvious reason for government agencies to combat fraud, abuse and improper payments is to save taxpayer money, it is equally important to maintain the public's trust by gleaning accurate information. The right technology helps government meet this goal by improving the effectiveness of audits and investigations, providing timely information for quick decisions and improving information credibility.

The stakes are high across government. Fraud, abuse and improper payments are an increasingly pervasive issue in government programs and result in hundreds of billions of dollars per year in losses. Here are just three examples of how pervasive fraud, abuse and improper payments can be:

- According to the IRS, its website for reporting fraud was visited more than 500,000 times in fiscal year 2011. A 2012 audit indicated that the IRS may lose $21 billion over the next few years due to identity theft alone.
- A 2012 cybersecurity study co-sponsored by the National Association of State Chief Information Officers (NASCIO) found that foreign state-sponsored espionage and external financial fraud have increased since 2010, while malicious software, hackers and physical attacks such as stolen mobile devices and Web threats continue to be a problem.
- A GAO report estimated losses to Medicare and Medicaid during 2010 at more than $70 billion, attributable to weak provider enrollment standards and procedures, poor pre- and post-payment claim review, and unacceptable contractor oversight, among other issues.

There are many methods, tools, applications and services to help combat fraud, abuse and improper payments. The UBM Tech survey found that fraud detection and alert generation were top priorities across the board both for the short and longer term. These two techniques consistently were rated above alert management/activity monitoring and business rules management, among others.

One of the study's participants who agreed to be interviewed about the results said he believes that part of the reason that fraud detection and alert generation came out on top is because of the media attention given to recent government fraud and abuse cases.

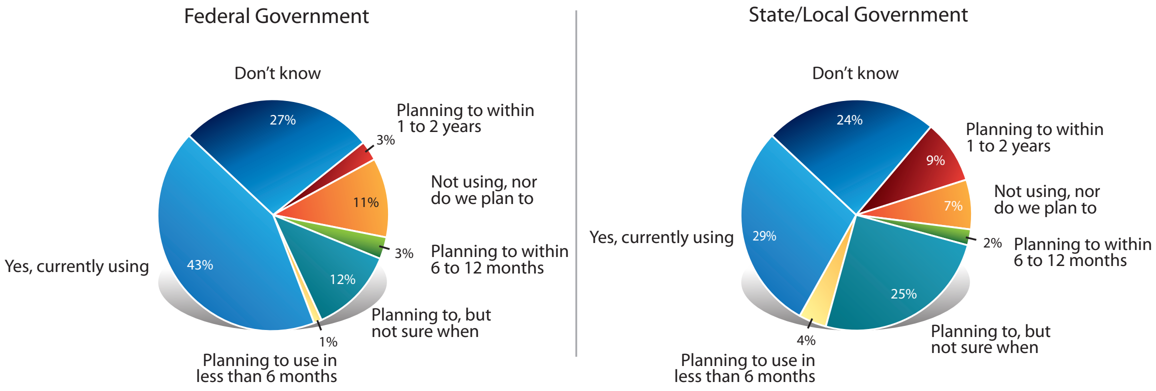
Also consistent among all survey participants were answers to a question about the benefits that agencies have seen from implementing fraud detection and prevention technology. The top two benefits were handling of new types of threats and reduction in the cost of combating fraud.

Fighting Back

The survey found that 43 percent of federal agencies are currently using technology for fraud prevention, versus 29 percent of state/local agencies (**see Figure 2**). The survey then followed up with those not using the technology to ask why. The top reason was the perception that the technology is too expensive — 36 percent on the federal side versus 71 percent on state/local. (For more insight into cost perceptions, see Cost vs. Benefit section below.)

Angie Petty, a senior principal analyst at Deltek, which conducts research on the government contracting market and recently did a study of its own, suspects that there are numerous reasons why federal agencies are further ahead than state and local agencies when it comes to fraud detection and prevention. She cited the growing number of federal mandates related to reducing fraud, abuse and improper payments; greater public visibility of the problem; the relatively larger amount of funds at risk; and in general,

Figure 2. Are you currently using or do you plan to use technology for fraud prevention?



Base: 105 federal government and 106 state and local government respondents
Data: UBM Tech survey of 211 government professionals, June 2013

larger IT budgets that allow agencies to shift priorities to find funds for implementation.

Agencies in Action

The IRS provides just one example of how an agency is using technology to fight fraud and abuse and reaping the benefits. The IRS is using data-mining tools to help stem the roughly 25 percent of claims for the Earned Income Tax Credit (EITC) that are paid in error. By using these tools to monitor accounts receivable, the IRS has been able to analyze tens of millions of EITC claims and flag those requiring further investigation. It uses the same techniques to analyze telephone tax refunds and fraudulent tax filings among prisoners. The IRS also plans to use the tools to examine more than 15 years of data in its Compliance Data Warehouse so it can better allocate its field and system resources.

Examples exist in state and local government as well. The Commonwealth of Kentucky, for example, uses predictive analytics to analyze eligibility and claims in Medicaid, food stamps and temporary assistance, with the goal of detecting and preventing fraud. Michigan uses predictive analytics to help identify fraud, waste and abuse in the state's unemployment insurance and food stamps programs, and plans to expand its use to other areas of government. And Los Angeles County is using advanced analytics and predictive models along with social network analysis to detect and prevent fraud in public assistance programs. Los Angeles County has uncovered hundreds of cases of child care fraud, and that success has spurred the county to expand its efforts to help fight fraud in its In-Home Supportive Services program.

While all of these programs have successfully fought fraud, abuse and improper payments, they also have saved the government agencies — and thereby taxpayers — significant money.

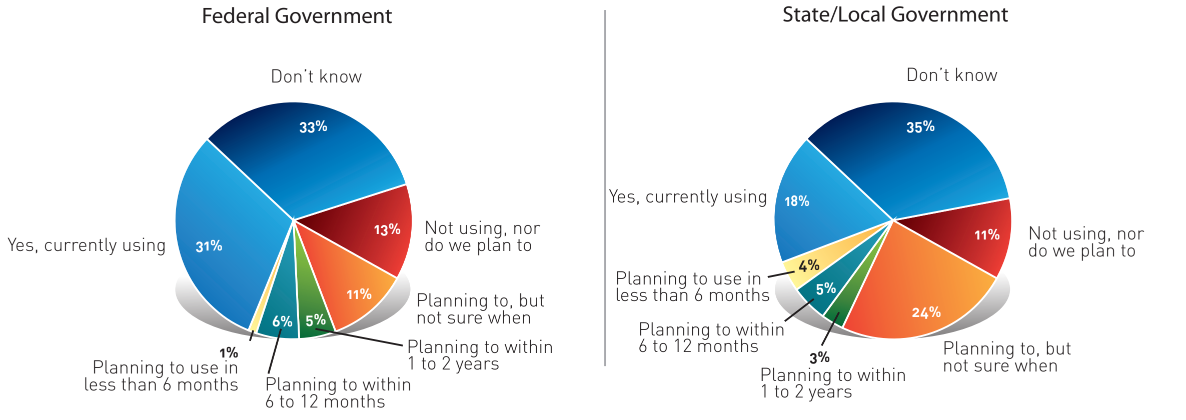
Both the IRS and Los Angeles County credit the technology with contributing to the savings of millions of dollars in inappropriate claims and activities that might otherwise go undetected. A housing authority in Austin, Texas, got even more specific: By implementing tools for fraud detection and alert generation, the agency has investigated and closed more than 2,900 cases of income fraud and unauthorized occupants and collected more than $1 million from fraud cases since 2004.

Technology Deep Dive

As demonstrated above, one of the most effective ways to help detect fraud, abuse and improper payments is through the use of advanced analytics and business rules. Advanced analytics is a statistical, quantitative or mathematical analysis of data to discover why something is happening, what will happen next and how to optimize actions so the desired results will occur. One of the most useful types of advanced analytics is predictive analytics, which analyzes current and historical data to predict future events.

The UBM Tech survey found that 31 percent of federal respondents are currently either using these tools or plan to, versus 18 percent on the state/local side (**see Figure 3**). Yet many more state and local agencies are planning to use these tools in the future (more than one-third), versus just 23 percent on the federal side. A nearly equal percentage said they don't know enough about advanced analytics (about one-third on both sides).

Figure 3. Does your agency or organization currently deploy advanced analytics or business rules to help detect fraud, or does it plan to?



Base: 105 federal government and 106 state and local government respondents
Data: UBM Tech survey of 211 government professionals, June 2013

One survey respondent surmised that the reason fewer state and local agencies are using analytics while many more plan to implement the technology is due to growing momentum.

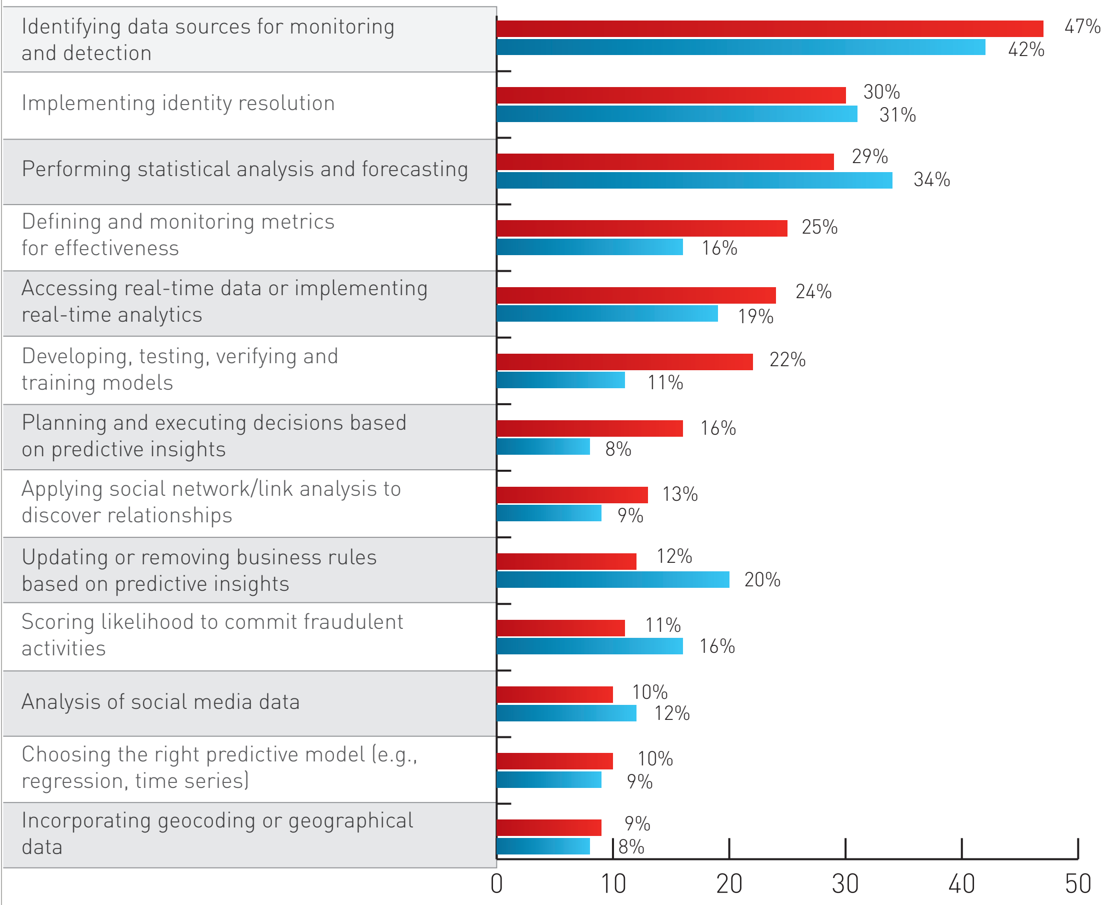
"State and local agencies have been capturing big data for eons, but they haven't been able to analyze it," he said. "But now that the analytics drumbeat has started and the tools are available, agencies are becoming more aware that there are tools that can help them look at structured and unstructured data."

When asked which advanced analytics, data mining or predictive analytics methods were being performed to combat fraud, abuse or improper payments, the highest percentage of respondents (47% of federal and 42% of state/local) said "identifying data sources for monitoring and detection" (**see Figure 4**). Close behind for all areas of government were "implementing identity resolution" and "performing statistical analysis and forecasting."

Continuous monitoring is another methodology that can help companies better manage risk and operate controls. Continuous monitoring is a process used to continuously review something against expected criteria and notify stakeholders when something out of the ordinary is detected. It is often used to ensure that processes, systems and operational key performance indicators are in compliance. In the tax arena, an example would be to continuously monitor tax records to look for abnormalities.

Failing to implement continuous monitoring can have serious consequences. One survey respondent recalled an incident in his county when the tax assessor's office failed to check property tax records for more than a decade. As

Figure 4. Which of the following items are you or those in your functional area performing as part of efforts to combat fraud, abuse and/or improper payments?



Note: Multiple responses allowed.
Base: 105 federal government and 106 state and local government respondents
Data: UBM Tech survey of 211 government professionals, June 2013

a result, the assessor and county manager were fired, and the county incurred millions of dollars in expenses to redo 2011 property assessments.

When asked whether they use or plan to use continuous monitoring technology, federal and state/local respondents responded markedly differently. Slightly more than half (51%) of federal respondents said they currently use the technology, versus 25 percent of state/local (**see Figure 5**). These respondents also indicated which metrics and indicators they view as most important when it comes to continuously monitoring fraud detection and prevention (**see Figure 6**). However, when asked about plans to implement continuous monitoring, 34 percent of state/local agencies responded that they planned to do so, versus 13 percent of federal. Nearly equal percentages said they don't know enough about continuous monitoring technology to make an informed decision.

The reason why the federal government is ahead in adopting both analytics and continuous monitoring to help stem fraud, abuse and improper payments may be due to the number of mandates and associated pressures that the federal government is placing on its agencies. These include:

- Executive Order 13520: Reducing Improper Payments and Eliminating Waste in Federal Programs. This order requires federal agencies to submit quarterly reports on any high-dollar overpayments identified in their high-risk programs to their respective Office of Inspector General and the Council of the Inspectors General on Integrity and Efficiency.
- Presidential Memo: "Finding and Recapturing Improper Payments." This memo requires executive departments and agencies to expand their use of payment recapture audits.
- Fraud Enforcement and Recovery Act of 2009. This act enhances criminal enforcement of federal fraud laws, especially with regard to financial institutions and mortgage, securities and commodities fraud.
- Improper Payments Elimination and Recovery Improvement Act of 2012. This act requires specific actions by the Office of Management and Budget, federal agencies and inspectors general regarding levels of oversight and reporting.

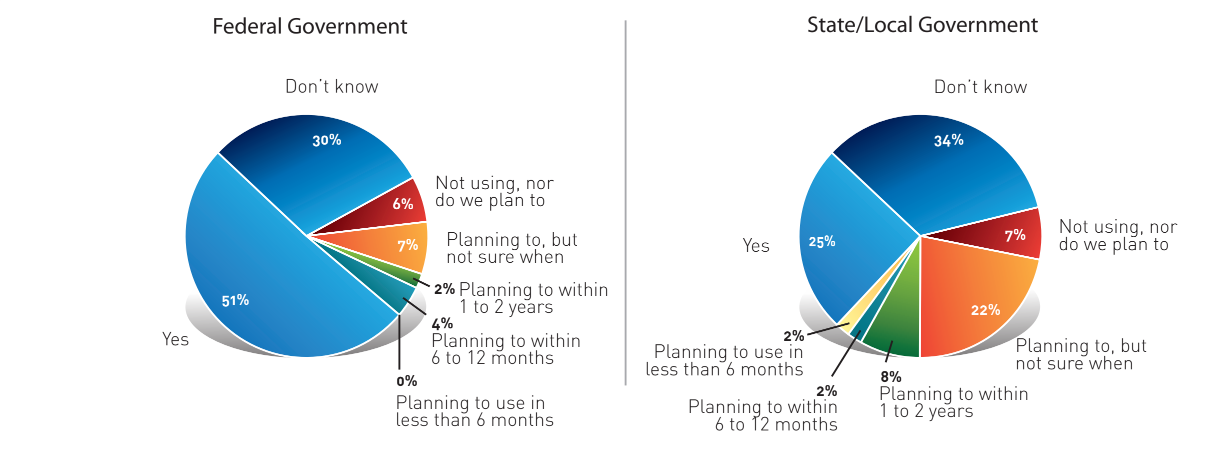
On the flip side, "there is only so much pressure the federal government can impose on state and local government to combat waste, fraud and abuse," analyst Petty said. "They have been successful in incentivizing states in the area of Medicare, but in other areas, it's really up to the states and municipalities themselves, and it can take more time for everything to trickle down."

A Steep Learning Curve

In many areas of the survey, UBM Tech found that a barrier to adoption of technology to help fight fraud, abuse and improper payments was simply not knowing enough about the technology. This came up over and over again:

- Roughly one-quarter of respondents (27% of federal and 24% of state/local) said they didn't know enough about fraud prevention to make an informed decision.
- About one-third (33% of federal and 35% of state/local) said they didn't know enough about advanced analytics and business rules to make an informed decision.
- Roughly one-third (30% of federal and 34% of state/local) said the same about continuous monitoring technology.

Figure 5. Does your agency or organization use or plan to use continuous monitoring technology?



Base: 105 federal government and 106 state and local government respondents
Data: UBM Tech survey of 211 government professionals, June 2013

Figure 6. Rank these metrics and indicators from most important to least important when it comes to continuously monitoring fraud detection and prevention.

	Federal Government		State / Local Government	
	Total Score	Overall Rank	Total Score	Overall Rank
Controls and control violations	338	1	339	3
Risk indicators	330	2	345	1
Operational processes and data	326	3	341	2
Business performance metrics	267	4	270	4
Exception remediation	166	5	186	5

Note: Score is a weighted calculation. Items ranked first are valued higher than the following ranks, the score is the sum of all weighted rank counts.
Base: 105 federal government and 106 state and local government respondents
Data: UBM Tech survey of 211 government professionals, June 2013

Cost Versus Benefit

Respondents also frequently cited cost as a barrier to adoption of fraud detection and prevention technology. For example, cost was a barrier for half of the respondents to adopting or planning to adopt fraud prevention technology. It also was considered the most challenging aspect of deploying or using fraud detection and/or prevention technology (49% of federal, 50% of state and local).

While cost concerns are understandable, it's quite possible that agencies aren't aware of how fast the payback can be once a fraud detection and prevention solution is implemented. A 2012 Nucleus Research study shows that organizations increase their return on investment as they increase their use of analytics. The study shows that enterprises achieve an average ROI of 188 percent in the initial automation phase, and an average of 1,209 percent in the later predictive analytics phase.

No matter what technology agencies use for fraud, abuse and improper payment detection and prevention — predictive analytics, continuous monitoring or other methods — savings can mount quickly. The Department of Health and Human Services and the Department of Justice's 2012 Health Care Fraud and Abuse Control Program Annual Report, for example, found that in fiscal year 2012, the federal government saved about $4.2 billion in healthcare fraud. A total of 826 defendants were convicted

Get Educated

While fraud detection and prevention are critical to agencies that want to stem fraud, abuse and improper payments at all levels of their organizations, it can be difficult to understand how the technology works and its value to the organization. It is definitely possible to gain that knowledge, however, through these methods:

- **Attend conferences.** One of the biggest bangs for the buck is attending a conference with a track on fraud, abuse and improper payments. These conferences generally feature experts and vendors discussing the technology. They often have breakout sessions and exhibit booths where you can learn more, and there is usually time to schedule one-on-one meetings with vendors or experts to gain more knowledge or learn more about a solution.
- **Read and interact online as much as possible.** Vendor white papers, online articles and blogs are all potentially valuable sources of information. Many online sources are interactive, allowing participants to ask questions.
- **Talk to other agencies.** Build relationships with agencies that have similar challenges and find out how they are using technology to tackle fraud, abuse and improper payments.
- **Invite vendors to your agency.** Vendors are more than willing to spend time educating people on how to use their technology most effectively.
- **Consult with industry experts.** Companies such as Forrester and Gartner follow the market and issue recommendations and insights regularly.

of healthcare fraud-related crimes during the year, and the Justice Department opened 885 new civil healthcare fraud investigations and had 1,023 civil healthcare fraud matters pending at the end of the fiscal year.

At the state level, Florida saved $6.80 for every dollar spent on fraud prevention and recovery and recouped nearly $50 million in total collections, mostly from overpayments. The state of Washington's Department of Labor and Industries expects an 8:1 return on investment and has seen an 80 percent increase in efficiency by using fraud detection and prevention technology. At the local level, Los Angeles County expects a return on investment of between $7 million and $30 million annually and has achieved 85 percent accuracy in identifying suspected fraud rings; and the Louisiana Workforce Commission expects an 8:1 ROI on its fraud detection and prevention technology.

While saving money may be top of mind for many agencies, there are many other factors that increase the ROI of a fraud detection and prevention solution. For example, results can be achieved much more quickly — and in higher volumes — than using manual methods, increasing the number of cases an agency can identify and investigate. The technology also can lead to greater staff productivity by reducing the number of leads that end up as dead ends, as well as reducing false positives.

Conclusion

Viewing the UBM Tech 2013 State of Fraud in Government survey clearly shows that agencies largely understand the importance of using technology to fight fraud, abuse and improper payments. Across the board, agencies understand that using technologies such as advanced analytics and continuous monitoring are the best ways to detect problematic issues.

At the same time, respondents voiced concern about the cost of implementing these technologies, and about not understanding their full capabilities. However, studies show that the return on investment of implementing these technologies is resoundingly positive, and there are myriad ways that agencies can learn more about them. Agencies that want to get ahead of the curve should take these steps:

- Prioritize projects for ferreting out fraud, abuse and improper payments.
- Dedicate a team focused on understanding the market and available technology solutions, including advanced analytics and continuous monitoring. Once team members understand the market, they can determine which solutions are best suited to achieving their agencies' goals.
- Narrow down choices to a short list and ask vendors to show how their technology can help them achieve their goals.

In the end, agencies that put in the time and effort to learn about technologies that effectively combat fraud, abuse and improper payments will be better equipped to deal with new types of threats, reduce the cost of combating fraud, abuse and improper payments, and predict the likelihood of fraudulent events or behavior. That can only be good for business. ◆

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 65,000 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®.

UBM Tech