

# WHY DATA IS YOUR KEY TO REDUCE WASTE, FRAUD & ABUSE



Sponsored by:  
**IBM**

The U.S. health care industry is losing an estimated



due to improper payments.

– **Paul Bermingham**, Executive Director,  
Xchanging Claims Services, Commentary: The  
Rise in Insurance Fraud and How to Combat it,  
Claims Journal, January 19, 2014.

# INTRODUCTION

*In partnership with IBM®, GovLoop is conducting a four-part guide series. Our reports will emphasize how big data has transformed government agencies and help you set a road map for adopting big data solutions. Here's what to expect in each chapter of our report.*

## **Chapter 1: Leveraging Your Most Critical Asset: Data**

In this section, we provided an overview of the current state of big data and the opportunity that big data analysis presents for government. Leveraging insights from the GovLoop community, we explored how agencies could capitalize on their most important asset: data.

### *IN THIS GUIDE:*

## **Chapter 2: Big Data's Role in Countering Fraud**

The second section of this report will explore how agencies can leverage data to improve fraud prevention methods. Growing use of the web for government transactions opens more areas to fraud. But with the proper tools and solutions, agencies can help combat fraud before it happens and be more efficient in service delivery.

### *COMING SOON:*

## **Chapter 3: Improving the Safety of Our Communities**

Agencies are looking at new ways to combat threats and keep communities safe. This means understanding how data can empower stronger insights and help prevent crime. With the use of analytics and robust data applications, agencies can improve the safety and economic vitality of their communities.

## **Chapter 4: How Data Analysis Powers Smarter Care**

Governments are looking for ways to improve how they deliver services to citizens and take a more holistic view of an individual. This requires a thorough understanding of the role of data. This section will explore how agencies are taking innovative approaches to using data to improve service delivery and support communities of care.

# CONTENTS

<b>To Face New Threats, We Need New Ways of Thinking</b>	<b>4</b>
<b>A New Approach to Counter Fraud – Before it Happens</b>	<b>5</b>
<b>Four Essentials: Detect, Respond, Investigate &amp; Discover</b>	<b>6</b>
<b>New York State – Using Data Analytics to Counter Fraud</b>	<b>7</b>
<b>A Smarter Approach to Counter Fraud</b>	<b>8</b>
<b>How to Get Started With Your Counter Fraud Strategy</b>	<b>9</b>
<b>Resources &amp; More Reading</b>	<b>11</b>
<b>Coming Soon: Transforming Public Safety with Analytics</b>	<b>12</b>



# TO FACE NEW THREATS, WE NEED NEW WAYS OF THINKING



In [our first chapter](#), we explained how big data has fundamentally changed the way government does business. But for many institutions, understanding the applications of big data is just the start of the analytics journey. In this chapter we dive deeper and focus on how deploying a data-driven approach to counter fraudulent activity can cut costs at your agency and help you deliver services more efficiently and effectively.

Today it is essential to remember that government agencies are collecting troves of transactional and behavioral data. If officials can understand the patterns, actions and processes behind these transactions, they can better understand their data as a means to combat fraud. We'll show you how throughout this chapter. Specifically you'll receive:

- An overview of IBM's approach to counter fraud.
- Insights from Carole Longendyke, counter-fraud client solutions professional at IBM, on how countering fraud is helping government become more efficient.
- An in-depth look at New York state's counter-fraud approach.
- Best practices to get started on your anti-fraud efforts.

Strategies to combat fraud come at an important time for government. As citizens demand more digital services, the risks of fraud, waste and abuse increase. Criminals have more outlets to attempt to compromise and obtain critical government information. Conspirators can use this data to commit acts of fraud, and because government services

are so complex, without a progressive and proactive information technology solution, agencies may never even know the depth of fraud, waste and abuse occurring. For instance, an [Internal Revenue Service investigation](#) found that a Louisiana woman submitted false reimbursement claims to Medicare for services that she had not administered. She was ordered to pay more than \$1.2 million in restitutions.

But not all thefts are detected and caught. People nationwide commit scores of tax evasion schemes and fraudulent white-collar crimes daily. The U.S. health care industry is currently [losing an estimated \\$180 billion per year](#) due to improper payments. On average, individual healthcare payers are losing 10 percent of their annual revenues to these improper payments. Advances in technology also enable deception schemes to be more sophisticated and perpetrators to more easily slip through the cracks.

But fraud is not just about financial issues; it is also about protecting consumer and proprietary data to build trust with customers. Government leaders now recognize the great opportunity their data holds in helping them spot abnormalities and stop tax and medical fraud, improper government payments, and insurance claims.

That's why IBM recently launched its ["Smarter counter fraud" initiative](#), leveraging IBM's expertise in analytics to combat waste, fraud and abuse in the public sector.

In our next section, Carole Longendyke, counter-fraud client solutions professional at IBM, tells us more about the company's approach to helping curb fraudulent activity.

# A NEW APPROACH TO COUNTER FRAUD – BEFORE IT HAPPENS



We all love a good detective story. Whether you tune into “NCIS” or “Law & Order” or leaf through the pages of a Sherlock Holmes story, you’re probably going to get hooked quickly. Within these stories, law enforcers attempt to solve crimes by interviewing suspects, gathering evidence, utilizing crime labs and putting everything together to find the perpetrators and bring them to justice.

But what if the crime was detected and stopped before it occurred? In the world of government counter-fraud strategy, predictive analytics aims to do just that.

Today, people use a myriad of digital technologies to engage with government organizations. Although these new tools have made it easier for government/citizen collaboration, making the government available round-the-clock on the web opens more areas to fraud. But with an anti-fraud strategy, agencies can combat scams before they happen and take a proactive stance to be more efficient in service delivery.

Countering fraud can rid agencies of unnecessary hassles and save millions – even billions – of dollars per year. However, such strategies aren’t one-size-fits-all. In fact, a poorly designed and implemented anti-fraud strategy could do more harm than good and excessively burden government systems and resources. “The key is in using smarter tools and resources in smarter ways,” said Longendyke, an IBM counter-fraud expert.

As criminals worldwide become more agile and sophisticated, governments must do the same. Big data plays a major role, and no efficient strategy can go without predictive analytics, collaboration and an inte-

grated approach to information management and sharing.

“When we talk about efficient and effective government, we think sensible use of resources that accomplishes goals without undue burden or roadblocks,” Longendyke said. “That means intercepting and stopping fraud, but also reducing or, to the extent possible, eliminating false positives in fraud detection.”

Predictive analytics is crucial in this respect. It uses a vast amount of data to detect serious risks without compromising mission impact or efficiency.

“Predictive analytics is a crystal ball, of sorts, in that it uses historical fraud data and statistics to anticipate fraudulent activities based on previously identified indicators,” Longendyke said. “Rules and fraud models are then applied in a decision environment where fraud points and thresholds are applied. Transactions or events that don’t exceed the statistical threshold can be confidently accelerated, thereby freeing resources to focus on those events that have a higher statistical relevance with respect to fraud.”

Put simply, predictive analytics uses fewer resources to accomplish more with greater accuracy and confidence. To consistently maintain this level of performance, IBM has developed four essentials to countering fraud. We explore them in our next section.





# FOUR ESSENTIALS: DETECT, RESPOND, INVESTIGATE & DISCOVER



*Detect, respond, investigate and discover are the four phases that represent the life cycle of IBM's Counter Fraud Management system. Longendyke describes this cycle as a "data ecosystem," in that it discovers, learns and multiplies its analytical resources to enable continuous growth in intelligence and improve functionality. The four phases create a smarter, more reliable system for counter-fraud management. We explore each below.*

## DETECT

The detect phase applies analytical fraud models and rules to the business process to determine if an action is potentially fraudulent before unnecessary deposits, withdrawals, transfers or payments occur. As new fraudulent schemes and schemers are discovered, the information and insights acquired are leveraged in this phase, where incoming data is compared to data previously associated with fraudulent activity and people.

## RESPOND

The respond component applies fraud insights to allow administrators to take action and confidently differentiate legitimate actions from suspicious ones by responding immediately to criminal patterns and activities. This is "where the rubber meets the road," Longendyke said. During this phase, safety officials should be able to prevent or interrupt suspicious actions by responding immediately to criminal patterns and activities. Take this scenario from Longendyke, for example:

"An auto insurance policyholder might submit several claims in a short period of time, soon after acquiring the policy or increasing his coverage. While these can be indicators of fraud, a finely tuned fraud response model will recognize indicators of fraud but also apply appropriate thresholds for actually labeling the claim as potentially fraudulent. In this example, a deeper dive investigation into this policyholder's claim would delay processing and ultimately damage customer satisfaction. But predictive analytics allows for smarter response to fraud indicators, thereby dramatically reducing false positives while increasing customer satisfaction and brand integrity."

## INVESTIGATE

The investigation stage turns fraud intelligence into action. Investigative teams perform and manage the deep inquiries into suspicious activity that will help compile evidence. This provides the thorough analysis required to build more compelling cases for prosecution and recovery or denial of payment. Supervisors, investigators, analysts and other team members are all connected in this effort, allowing for collaboration and an integrated, streamlined workflow. Rapid assessment and response means greater efficiency and effectiveness of the counter-fraud efforts, which results in faster resolutions of the investigations and lighter workloads.

## DISCOVER

While in the discover component, organizations can use a rich set of analytic capabilities to identify suspicious activity by reviewing historical data, analyzing patterns and building watch lists to categorize individuals or organizations that might be conducting fraudulent activities.

"This is the part that enables us to stay ahead of the game where fraudsters are concerned," Longendyke said. The powerful analytic capabilities embedded within the system identify new instances of fraud not previously detected. That information then becomes a part of the fraud models, which in turn are deployed in the detect phase.

To get a better idea of the application of this counter-fraud system, we examine several case studies below. Each scenario illustrates how data and analytics can greatly improve fraud detection and service delivery efficiency.

# NEW YORK STATE – USING DATA ANALYTICS TO COUNTER FRAUD



Rochester, NY

*In Chapter One, we briefly explained how Nonie Manion, executive deputy commissioner of New York's Department of Taxation and Finance, used analytics to improve how refunds were disbursed. Below is the full case study on the transformative work she and her team have done.*

## **"Fraud and falsehood only dread examination. Truth invites it."**

This quixotic statement from American economist and political philosopher Thomas Cooper praises honesty and fair play, while promising that the system will catch those who try to manipulate it. But in reality, the many cases of fraud and delinquency plaguing the American tax system counter Cooper's belief.

Companies and individuals collect millions of dollars each year in undue tax returns. This causes many to think that maybe fraud doesn't "dread examination" but rather evades it. To effectively detect questionable tax returns, auditors and agencies need to play smarter and harness the power of analytics.

At New York state's Department of Taxation and Finance, Nonie Manion, Executive Deputy Commissioner, has a mission to secure fairness through vigilance for the American taxpayer. Unlike her predecessors, who rose through the ranks of auditors, Manion comes from an IT background; she previously created applications for the auditor division.

Manion's foundation brought a fresh perspective to the department. She introduced the pivotal role that data-driven decisions would play in the department's processes. The key to accurately identifying

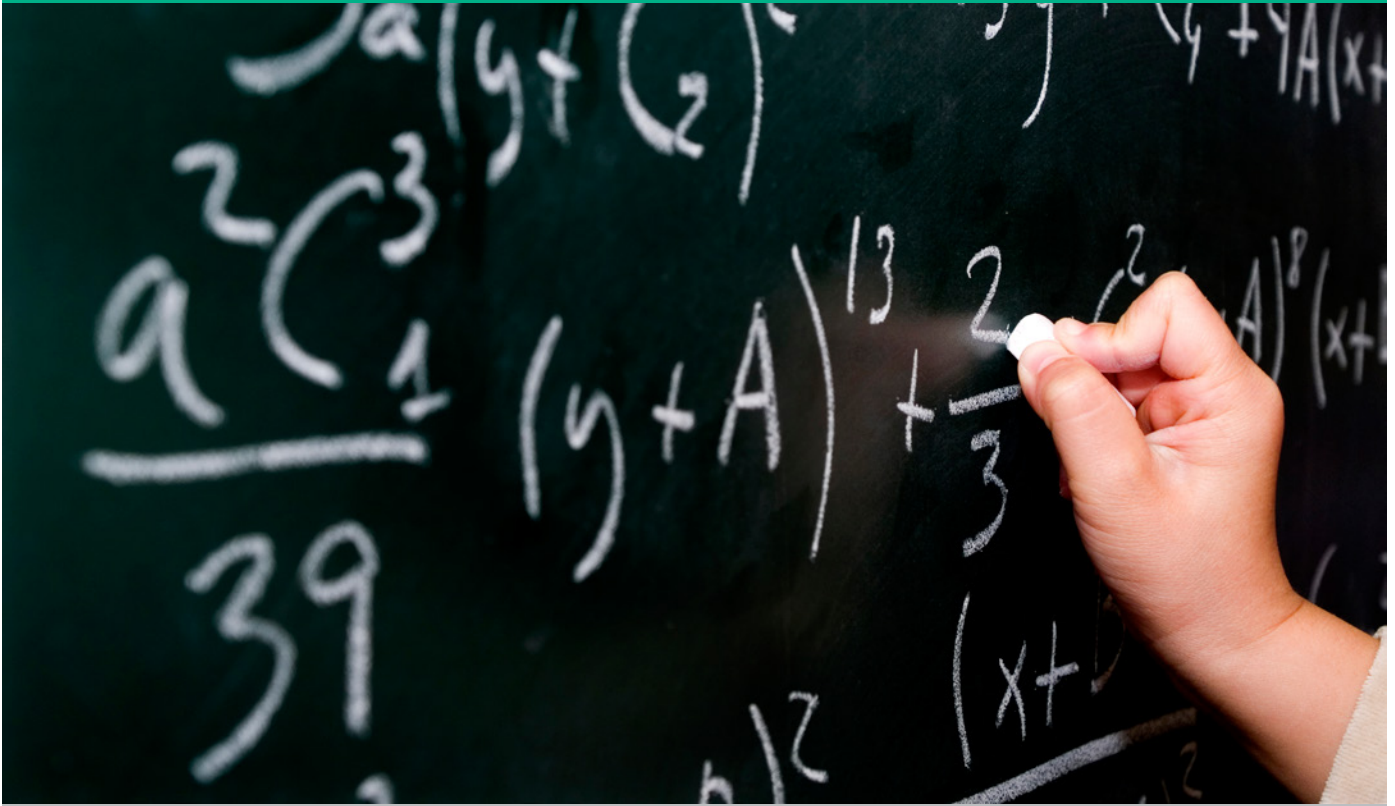
questionable tax returns and keeping taxpayers accountable, she said, is to incorporate more data sources with the use of predictive intelligence analytics.

Per Manion's influence, NYS Tax changed its vision in 2010 and adopted an intelligent tax screening solution from IBM called Case Identification and Selection System (CISS). As opposed to the department's previous system – which could detect faulty refund checks only after they had been sent out – CISS operates on an integrated, proactive basis. It places data analytics directly into the tax return process, allowing NYS Tax to use predictive intelligence to flag or refuse suspicious refund requests.

CISS has revolutionized the department's auditing process. For instance, it decreased the revenue drain that questionable refunds caused by \$1.2 billion in 2010 alone. In addition, tax collections increased by more than \$100 million. The organization's success has sparked interdepartmental interest in collaborative efforts and finding new opportunities to use analytics.



# A SMARTER APPROACH TO COUNTER FRAUD



During one of GovLoop's recent online trainings, [A Smarter Approach to Counter Fraud](#), industry and government experts joined to discuss counter-fraud strategies. The panel included:

- Nonie Manion, Executive Deputy Commissioner, New York State Department of Taxation and Finance.
- Ed Rounds, Industry Smarter Solutions Team Fraud and Crime Solution Leader
- Jonathan Turner, Senior Director of Global Compliance Investigations at Wright Medical Technology.

Rounds stressed the need for an adaptable approach since fraudsters' methods change so frequently. "The more data you can capture means the larger the observation space, which leads to better analytics, which leads to less breaches," he said.

Turner discussed taking a holistic approach to catching anonymous hackers. To stop them, he said, agencies "must use a range of different tools in order to recognize patterns. You can't focus on one particular solution."

Manion warned that tax collecting agencies must maintain positive public relations and keep pace with the changing times. "Our mantra used to be just to 'collect revenue' and today it's to 'efficiently collect the revenue with proficiency and integrity,'" she said.

The three discussed how hackers can access internal data more easily than one might think. "Criminal networks target organizations to learn their limits," Rounds said. Once preliminary knowledge is gained, attackers use this information to find loopholes and design an attack to compromise information.

Manion has used innovative tactics to combat internal worries. It's a fine line between monitoring valuable data and invading employee privacy rights, but with so much information accessible, it would be naïve not to keep track of it. Her branch has designed "selfie" accounts in which managers can see mirror screens of employees to look for suspicious activity.

The panel also agreed on the multitude of reasons why companies should become more focused on countering fraud. Rounds emphasized how the goal is more significant than just cutting wasteful spending.

The public is sometimes primed to think an event will occur if it's made salient in the media even though it's not always accurately portrayed. "To truly assess risk we need to measure the likelihood of fraud taking place, the financial impact, and then other insularly impacts of fraud," Rounds said.

Analysis paralysis is often an organization's worst enemy. Everyone should begin their counter-fraud program now regardless of their resources, Turner said.

"Take anti-fraud steps and build with what you have," he said. "You don't need a perfect system, just a better one than you have today."

"The biggest challenge is overcoming self-defeat, Turner added. "The sense of denial on the front end can be toxic." In a world where hackers will stop at nothing to create fraud, your best game plan is creating a defense, perfect or not.



# HOW TO GET STARTED WITH YOUR COUNTER FRAUD STRATEGY



*Below is a lightly edited transcript of an interview with counter-fraud expert, Carole Longendyke.*

**GovLoop:** Getting started with a counter fraud strategy isn't easy. How should government agencies begin?

**Longendyke:** As a start, I'd say it's important to know the risks specific to the industry and then the vulnerabilities specific to the organization. This is essential for assessing the scope of the required counter-fraud measures.

Too little and too much are both bad. Organizations need to first acknowledge responsibility for fraud detection and prevention, then develop a strategy, and allocate resources to implement the strategy. Those are the high-level bullet points to consider, but of course the devil is in the details. And with counter fraud, the critical details lie with the strategy. I would say that one particularly critical element is the role analytics plays in fraud detection. It's smart to mitigate fraud effectively, but smarter to proactively anticipate and stop it in the first place.

Analytics allows us to see trends and patterns before they become obvious. Compare this to the practice of auditing for fraud, which is still widely used for fraud detection. The auditor is looking at what has already occurred. Analytics lets us use that information to see into the future, so to speak.

I'll give you a very simple example. During the days leading up to the start of the Moscow Olympics, there was tremendous concern about the potential for terrorism. Intelligence investigators and analysts used a widely available source of data and applied simple principles of analysis, and were able to proactively identify and stop would-be demonstrators from organizing. How did they do that? Twitter.

The protest organizers tweeted anonymously, but to the investigators looking to prevent incidents, the information that mattered more than individual identities was the trends and patterns that would have only been discovered through data analysis. A spike in the use of an otherwise innocuous word catches our attention and tells us this is something that deserves closer scrutiny. In Moscow, analysts were able to determine where and when potentially violent events were to occur, and proactively respond. Again, this is a very simplified example, but the point to remember is that data analytics is the greatest resource we have for fighting fraud, and should therefore be high on the list of best practices.



# ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 140,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to [info@govloop.com](mailto:info@govloop.com).

GovLoop  
1101 15th St NW, Suite 900  
Washington, DC 20005

Phone: (202) 407-7421 Fax: (202) 407-7501

[www.govloop.com](http://www.govloop.com)

Twitter: [@GovLoop](https://twitter.com/GovLoop)

# ACKNOWLEDGMENTS

Thank you to IBM for their support of this valuable resource for public-sector professionals.

## Authors:

Patrick Fiorenza, GovLoop's senior research analyst

Mallory Thayer, GovLoop's research fellow

Matthew Garlipp, GovLoop's research fellow

## Designers:

Jeff Ribeira, GovLoop's senior interactive designer, and  
Tommy Bowen, GovLoop's junior designer.

## Editor:

Catherine Andrews, GovLoop's director of content



# ABOUT IBM

The world isn't just getting smaller and flatter, it is also becoming more instrumented, inter-connected and intelligent. As we move toward a globally integrated economy, all types of governments are also getting smarter.

IBM® provides a broad range of citizen centered solutions to help governments at all levels become more responsive to constituents, improve operational efficiencies, transform processes, manage costs and collaborate with internal and external partners in a safe and secure environment.

Governments can leverage the unparalleled resources of IBM through IBM Research, the Center for the Business of Government, the Institute for Electronic Government and a far-reaching ecosystem of strategic relationships.

IBM®, the IBM logo, ibm.com, are trademarks or registered trade-marks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM® trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or TM), these symbols indicate U.S. registered or common law trademarks owned by IBM® at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM® trademarks is available on the Web at "Copyright and trade-mark information" at: [IBM.com/legal/copytrade.shtml](http://IBM.com/legal/copytrade.shtml). Other product, company or service names may be trademarks or service marks of others.

# MORE READING

- [Using Data Analytics to Counter Fraud: New York State Tax Case Study](#)
- [A New Approach to Counter Fraud](#)
- [Keys to Counter Fraud: Detect, Respond, Investigate and Discover](#)
- [An Apple a Day Keeps the Fraudsters Away](#)
- [To Face New Threats, We Need New Ways of Thinking](#)
- [Social Cast: New threats. New thinking. A smarter Approach to Countering Fraud.](#)
- ["IBM Counter Fraud Management for Government: Detecting, identifying, and reducing tax fraud, while improving compliance"](#)
- ["IBM Counter Fraud and Improper Payments for Government: Detect, respond and reduce improper payments for Health and Human Services"](#)
- ["Tax revenue management and economic vitality: Using technology and data to maximize government revenue"](#)

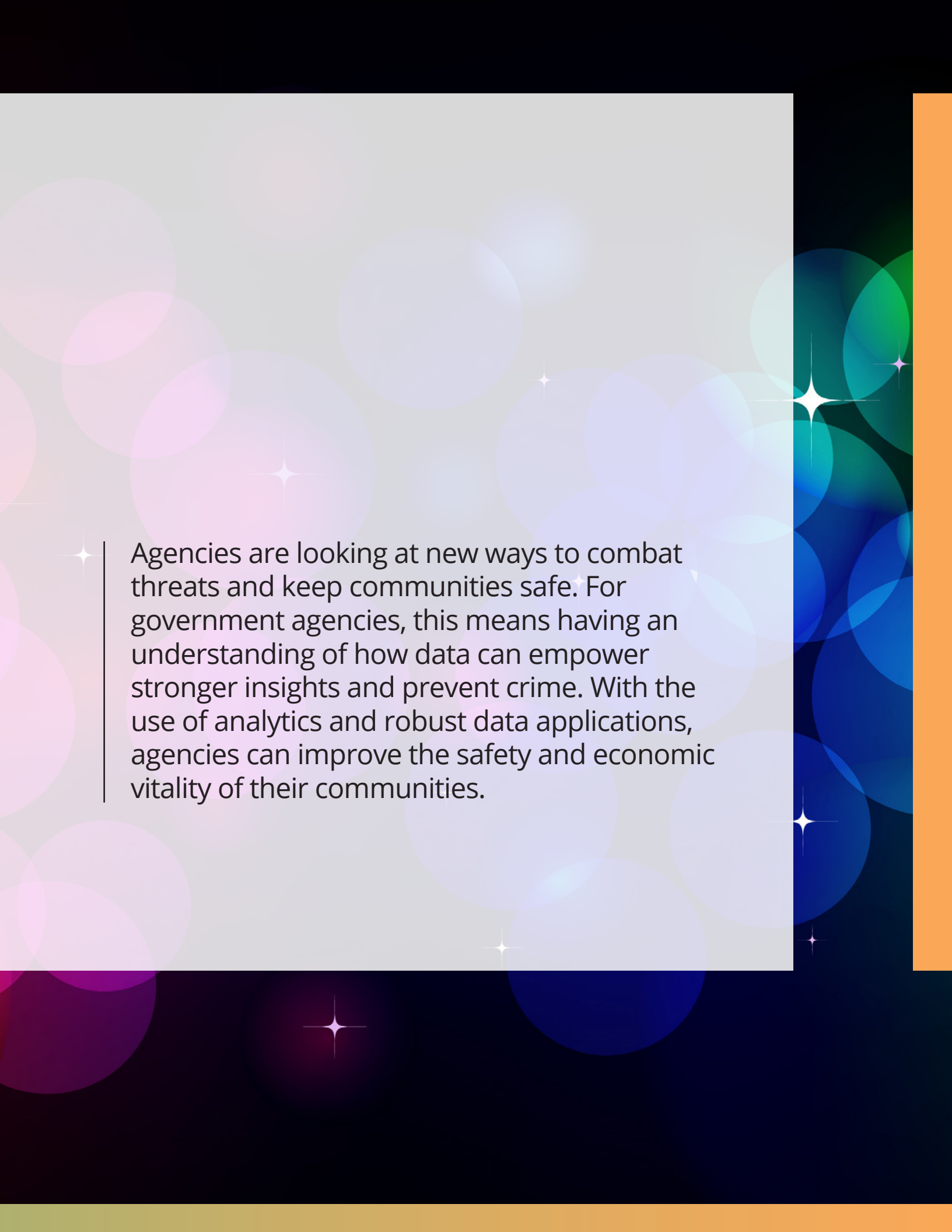




# Coming Next: Transforming Public Safety with Analytics





The background features a dark blue gradient with a pattern of overlapping circles in shades of pink, purple, and blue. Several white starburst or spark-like graphics are scattered across the design. A solid orange vertical bar is positioned on the right side of the image.

Agencies are looking at new ways to combat threats and keep communities safe. For government agencies, this means having an understanding of how data can empower stronger insights and prevent crime. With the use of analytics and robust data applications, agencies can improve the safety and economic vitality of their communities.



Sponsored by:



GOVLOOP  
1101 15TH ST NW, SUITE 900  
WASHINGTON, DC 20005  
PHONE: (202) 407-7421 | FAX: (202) 407-7501  
[WWW.GOVLOOP.COM](http://WWW.GOVLOOP.COM)