Deloitte
University
Press

Shutting down fraud, waste, and abuse

Moving from rhetoric to real solutions in government benefit programs

About the authors

Peter Viechnicki

Peter Viechnicki is a strategic analysis manager and data scientist with Deloitte Services LP, where he focuses on developing innovative public sector research using geospatial and natural language processing techniques. Follow him on Twitter @pviechnicki.

William D. Eggers

William Eggers Eggers leads public sector research for Deloitte. His new book, Delivering on Digital: The Innovators and Technologies that are Transforming Government, will be published in June 2016. His commentary has appeared in dozens of major media outlets including the New York Times, Wall Street Journal, and the Chicago Tribune. He can be reached at weggers@deloitte.com or on twitter @wdeggers.

Brien Lorenze

Brien Lorenze is a principal in the Regulatory, Forensics & Compliance practice of Deloitte Transactions and Business Analytics LLP and the Advisory global public sector leader. He is recognized for his industry knowledge, application of information technology to complex challenges, and as a leader in applying analytics to monitor/detect money laundering, fraud, and sanctions evasion.

Michael Greene

Michael Greene is a senior manager and data scientist with Deloitte Consulting LLP. He focuses on helping public- and private-sector organizations solve complex issues with predictive analytics and behavioral science.

James Guszcza

James Guszcza is the US chief data scientist for Deloitte Consulting LLP. He is the author of dozens of articles on analytics, including "The last-mile problem: How data science and behavioral science can come together."

Dan Olson

Dan Olson, CFE, a senior manager with Deloitte & Touche LLP, has worked for over 20 years in health care fraud examination following five years in auditing and compliance. Olson serves as a content specialist in the design and deployment of health care fraud, waste, and abuse predictive models and predictive analytics. Among his accomplishments, Olson has authored five health care white papers and testified before Congress regarding recommendations to identify health care fraud, waste, and abuse.

Contents

Introduction

FRAUD, waste, and abuse." A simple Google search returns about 35 *million* mentions of this term.

It's not surprising. For decades, our political leaders have promised to cut fraud, waste, and abuse from government spending, but somehow the problems persist, draining billions—some estimates would say trillions[1]—of taxpayer dollars.

In the 2015–2016 election season alone, several presidential candidates have made cutting fraud, waste, and abuse a key part of their platforms. Blue-ribbon commissions and bipartisan panels from California to Wisconsin have vowed to tackle the problem.[2] None of these, however, have managed to cool the hot rhetoric around the topic.

Or rewind to 2012, the year in which President Barack Obama asked Vice President Joe Biden to spearhead a "campaign to cut waste" that would "hunt down and eliminate misspent tax dollars in every agency."[3] The goal: Restore citizen trust in government.[4]

During the 1996 presidential campaign, Senator Bob Dole mentioned government waste at least 33 times, and promised to fund his proposed tax cuts with a scalpel: "There's enough waste in the government to give you the tax cut, enough waste, enough fraud, enough abuse, enough people flying around the world …"[5]

In 1982, Ronald Reagan asked investigators to "work like tireless bloodhounds" to "root out inefficiency."[6] Calling fraud, waste, and abuse "the byproduct of mismanagement," Reagan said, "Our management improvements, together with the tremendous accomplishments of our Inspectors General, are a one-two punch taking steam out of the waste and fraud that was eroding faith in our government."

And way back in 1949, President Truman directed ex-President Herbert Hoover to organize 300 men and women to seek waste in what Hoover called "the most formidable attempt yet made for independent review … of the Executive Branch." Such investigations, he noted, happened periodically at least "since the Taft Administration."[7]

Yet despite decades of pledges, campaigns, and thick reports, the challenge remains. The Government Accountability Office recently announced it found $137 *billion* in improper payments in 2015, an increase of $31 billion in just two years.[8]

Politicians have been promising to win the war on fraud, waste, and abuse for about as long as we've had voters. But the disappointing outcomes suggest they still haven't found a strategy that works.[9]

This study sidesteps the tired rhetoric to present a realistic, proven approach for reducing fraud, waste, and abuse, and debunks some common myths along the way. Our approach borrows from commercial leading practices to approach fraud at an enterprise level, while also incorporating new methods from social science. If the private sector's experience is any guide, the fixes we propose here won't happen overnight, but the progress they offer could be game-changing.

We urge agencies to cut across silos and use new tools and techniques, such as predictive analytics, behavioral economics, and collective intelligence, to reduce system-wide vulnerabilities. Redesigned systems can reduce the chances of wasting funds in the first place. By creating an ecosystem in which the incentives of all stakeholders align to prevent fraud, waste, and abuse, the government can begin to drain the sources of a perennial problem.

Before diving deeply into these new solutions, however, it's important to first understand the nature of the challenge—fraud, waste, and abuse in government benefit programs—and the ways in which they have endured despite decades of effort.

Seeing fraud, waste, and abuse clearly

BERRI Davis has a daunting mission. She's one of the directors of a program integrity team at the Government Accountability Office (GAO), charged with auditing all federally funded benefits programs, including enormous programs such as Medicaid and Social Security.[10] Davis and her colleagues work with federal agencies and states to improve program integrity by identifying vulnerabilities and recommending fixes.

Davis's team, with its bird's-eye view of billions of dollars wasted or stolen annually from benefits programs, faces a task that could easily become overwhelming. Fortunately, she and her GAO colleagues have an important asset: They can rely on almost 10 years' worth of data to assess the size and scope of improper payments in various programs.[11]

The 2002 Improper Payments Information Act (IPIA) requires federal agencies to measure and report on improper payment rates in their benefits programs.[12] In response, agencies have developed methods such as the Centers for Medicare & Medicaid Services's (CMS's) Payment Error Rate Measurement (PERM) program.[13] Data produced by PERM and similar programs over the past 10 years show the fluctuations in improper payments[14] which themselves reflect the dynamic nature of fraud, waste, and abuse.

Our analysis of the data produced under IPIA, together with interviews with numerous federal and state integrity officers, reveals the landscape of fraud, waste, and abuse in benefits programs. With these data, we can examine the extent and scope of losses as well as trends and recovery amounts.

The size of the challenge

The Congressional Research Service estimates that the federal government allocated nearly $2.1 trillion for mandatory expenditures in 2014, mostly for benefits programs.[15] How much of that enormous sum was lost to fraud, waste, and abuse? For 2015, the White House estimated a loss of $137 billion through improper payments.[16]

Some expenditures, such as those for health programs, may be particularly prone to fraud, waste, and abuse. The most rigorous available assessments of overall waste in health spending have placed it in the range of 30 percent.[17]

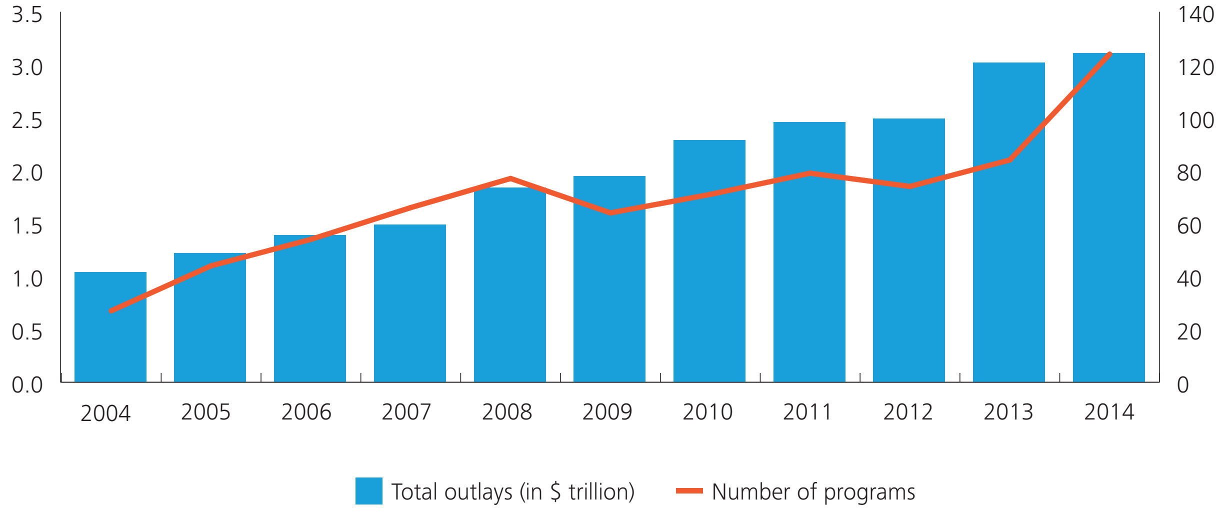
Of course, fraud implies *intention*—a deliberate act. Many other improper payments represent waste and error. If a doctor's office bills a higher-level procedure code without the required documentation, it does not necessarily mean that it was intentional.

Improper payments data aren't designed to measure fraud directly because they can't assign or assess intention. Claims analysis can identify repeated trends and patterns that appear suspicious. To identify fraud, intent needs to be established—which moves beyond traditional claims analysis and involves a human element to confirm the behavior that was exhibited.

Better reporting boosts improper payment numbers

At first glance, the improper payments figures tell a dismal story. Total improper payments reported by government benefits programs rose from $38 billion in 2005 to $137 billion in 2015, a 197 percent increase in inflation-adjusted dollars over 10 years.[18]

Figure 1. Growth in total program outlays tracked and number of programs reporting improper payments



Source: US Office of Management and Budget, *Office of Federal Financial Management improper payments dataset*, https://www.whitehouse.gov/omb/financial/improper_payment_dataset; Government Accountability Office, *Government-wide estimates and use of death data to help prevent payments to deceased individuals*, March 16, 2015, p. 1, http://www.gao.gov/assets/670/669026.pdf; and Government Accountability Office, *Government-wide estimates and reduction strategies*, July 9, 2014, p. 1, http://www.gao.gov/assets/670/664692.pdf.

Graphic: Deloitte University Press | DUPress.com

But much of the apparently sharp increase actually resulted from two factors: One, more agencies are finally reporting their improper payments accurately (figure 1)[19] and two, analytic techniques are getting better at detecting underlying problems that lead to improper payments. As Carolyn Yocom, a GAO colleague of Berri Davis, notes: "Not all increases in improper payments are bad news, as an increased rate can be due to agencies' improvements in measuring improper payments and taking steps to combat them."[20]

Despite some gaps, our store of improper payments data is becoming more comprehensive every year.[21]

Many programs are still establishing their procedures for estimating unnecessary expenditures. But we can finally begin to understand the scope of the problem.

And it's clear that improper payment rates remain staggeringly high, particularly for big-ticket benefits programs. Figure 2 provides improper payment amounts for seven large programs tracked under the Improper Payments Act. Together, these seven programs lost more than $115 billion through improper payments in 2015 alone.

Fraud is dynamic

Because the nature of fraud itself is changing, program integrity officials at the GAO aren't expecting victory any time soon. And 3,000 miles away from the capital, a pair of recent high-profile cases have revealed some troubling trends.

Jamie Ralls and Ian Green are certified auditors with the Oregon Secretary of State. They and a dedicated team of about 70 colleagues are on the lookout for fraud, charged with confirming that the state's tax dollars are being spent for their intended purpose. Their office has audit authority over the entirety of Oregon's $69 billion budget, including more than $21 billion in federal funds.[22]

The recent exposure of a massive food-stamp fraud ring in Klamath Falls, Oregon, shows just how quickly the problem of benefits fraud and abuse can change.

The first hints that something was amiss in Klamath Falls came in 2012, when an Oregon

Figure 2. Improper payments in large benefits programs, 2005–2015

Program	Total outlays in 2015 (in $ billion)	Improper payment rate in 2015	Total improper payments in 2015 (in $ billion)
Medicare Fee-for-Service	358.3	12.1%	43.3
Medicaid	297.7	9.8%	29.1
Earned Income Tax Credit (EITC)	65.6	23.8%	15.6
Medicare Advantage (Part C)	148.6	9.5%	14.1
Old Age, Survivors and Disability Insurance (OASDI)	862.7	0.6%	5.0
Supplementary Security Income (SSI)	56.5	8.4%	4.8
Unemployment Insurance (UI)	32.9	10.7%	3.5

Source: Office of Management and Budget, *Office of Federal Financial Management improper payments dataset*.

Department of Human Services caseworker heard from a food-stamp recipient that the local market Carniceria Mi Pueblo was making fraudulent sales to beneficiaries in return for cash payouts.[23] State officials began examining food-stamp transactions from the Carniceria and noticed a series of red flags. These small-scale infractions led to a criminal ring that laundered an estimated $20,000 each month in food-stamp benefits and had links to Mexican drug cartels. Two years later, police arrested 65 people in connection with the case.[24] The ensuing headlines generated opinions ranging from approval for public officials' hard work to condemnation for the two years it took them to act.[25]

Oregon anti-fraud officials probably also took notice of a 2013 case of Medicaid fraud in neighboring California, which highlighted how would-be fraudsters are joining forces to form criminal networks. The network in question stole millions of dollars from California's Medi-Cal program by convincing nonaddicted residents of group homes to participate in addiction therapy sessions.[26] The participants received cash, cigarettes, and snacks, while the state kept paying providers for the sessions. Following this discovery, scrutiny of organized crime networks became an integral part of Medi-Cal's integrity efforts.

Both cases make it clear that dishonest actors are applying more sophisticated methods to perpetrate fraud. In fact, would-be fraudsters continually probe benefits systems to identify vulnerabilities—and then move to exploit them.[27]

For states such as Oregon and federal agencies as well, the inevitable move to digital technologies has created new opportunities for fraud, including large-scale identity theft. In 2012, some 12.6 million Americans became victims of identity theft, and 46 percent of these cases involved government documents or benefits fraud.[28] Benefits fraud is often combined with identity theft, providing a strong economic incentive for thieves to steal identifying information.

As benefits administration shifts from brick-and-mortar locations to web-based transaction systems, interactions between beneficiaries and administrators become less personal, creating more space for small acts of dishonesty; it's easier to lie to a computer than to a person. Psychologist Dan Ariely has called this "the personal fudge factor."[29]

Government agencies can't buy their way out of the problem

The current fiscal climate means that states and federal agencies cannot respond to rapidly changing trends in fraud and abuse simply by increasing funding for fraud prevention.[30] Public budgets for prevention and enforcement are either flat or declining. Budgets for auditors and inspectors general are particularly vulnerable, since they're often viewed as partisan political targets, with little recognition for their positive returns on investment.[31]

Instead, those fighting fraud will have to innovate within their existing budgets. To be successful, their efforts will require a more holistic approach, one that spans the enterprise of government and employs new tools and techniques, from predictive analytics and deep learning to behavioral "nudges" and collective intelligence.

A holistic approach to waste and fraud reduction

THERE'S no single solution to the problem of fraud, waste, and abuse. Because the problems are complex and evolving quickly, any effective solution must be both multifaceted and agile.

Fortunately, 20 years of successful fraud reduction in the private sector has shown that program vulnerabilities can be mitigated with an enterprise approach that combines retrospective and prospective approaches, predictive analytics, and adaptive techniques such as machine learning and randomized controlled trials. (Figure 3 illustrates such a system.) Five strategies in particular are critical:

- Make data collection central to anti-fraud and waste strategies
- Create a learning system to respond to ever-changing threats
- Emphasize prevention to get the best return on effort
- Use "choice architecture" to encourage compliance
- Share intelligence to reduce intentional fraud

Make data integration central to anti-fraud and waste strategies

Most readers aren't terribly excited by extensible database architectures or enduring data-sharing agreements. But these are *just* the sorts of features needed to plug holes in benefits programs. Due in part to small but significant improvements in data sharing and data matching, improper payment rates in the Supplemental Nutrition Assistance Program (SNAP) have been pushed down from a high of 6.0 percent in 2007 to its lowest level ever, 3.2 percent, in 2014.[32]

Data collection is *critical* to the prevention of fraud, waste, and abuse. It should begin with the identification of relevant data sources and a robust process for acquiring data and compiling them into a dynamic data warehouse. Such data might include information about applicants and current beneficiaries; information from other government systems about the same individuals; and data on current and past claims. Such data may come from external sources: other benefits programs, other agencies and states, and even social media.

As these data are assembled, the system acquires enough information to make informed decisions about incoming claims, applications, and other transactions through risk-scoring.

Create a learning system to respond to ever-changing threats

Adaptive enterprises learn from interaction with data and humans, continuously reconfiguring in pursuit of better outcomes. This adaptive strategy is crucial to effective program integrity platforms.

All too often, leaders think of program integrity systems as a fixed defense, like a wall. But a Great Wall can be scaled; a Maginot Line can be avoided. Fixed obstacles are fixed targets. That's not optimal defense. Instead, think of the fight against fraud as a chess match.

Governments must deploy their advantages and strengths against their opponents' disadvantages and weaknesses.

Twenty years of best practices in private-sector fraud prevention show that perpetual unpredictability is the best defense against benefits fraudsters.[33] The goal is to modify defenses so fast that adversaries are continually playing catch-up. The more you change the game, the more the fraudsters' costs go up, and the more your costs go down. Maybe they'll move on to a different target.

A system that can learn from its own experiences requires an offline component that collects outcomes and uses them to manage and update rule bases and statistical models using new training data (figure 3). Business rules and anomaly detectors are updated based on incoming transactions as well as external information. Such a system is adaptive because it learns both from the effects of its own actions and from external data, including the wisdom of crowds.

This knowledge base can be used to assign a risk score to each incoming transaction. Transactions that match a normal risk profile are processed with little manual intervention. Those that stand out in some way are assigned a high risk score and sent for further investigation or immediate action.

Successful systems also measure the effectiveness of each action taken, and adjust actions based on those results. A/B testing of potential interventions, discussed below, can reveal which ones have more impact on desired outcomes, such as more accurate beneficiary data.

Emphasize prevention to get the best return on effort

Many public benefits programs approach fraud, waste, and abuse with a "pay-and-chase" model. They focus on clawing back money paid out on fraudulent claims after the fact, and pay less attention to the potentially more lucrative categories of waste and error. We say more lucrative because fraud typically accounts for a third or less of all improper payments. Deliberate fraud in the unemployment insurance program, for instance, constitutes 28 percent of overpayments.[34] Fraudulent recipient claims in SNAP account for just 10 percent of overpayments.[35] And potentially fraudulent claims in California's Medi-Cal fee-for-service program made up 37.8 percent of all erroneous payments in 2011 ($473 million of $1.25 billion), which themselves comprised 6.05 percent of all FFS payments.[36]

A prevention-focused strategy can be doubly lucrative: Prevention saves not just the cost of overpayments, but also the cost of the chase.

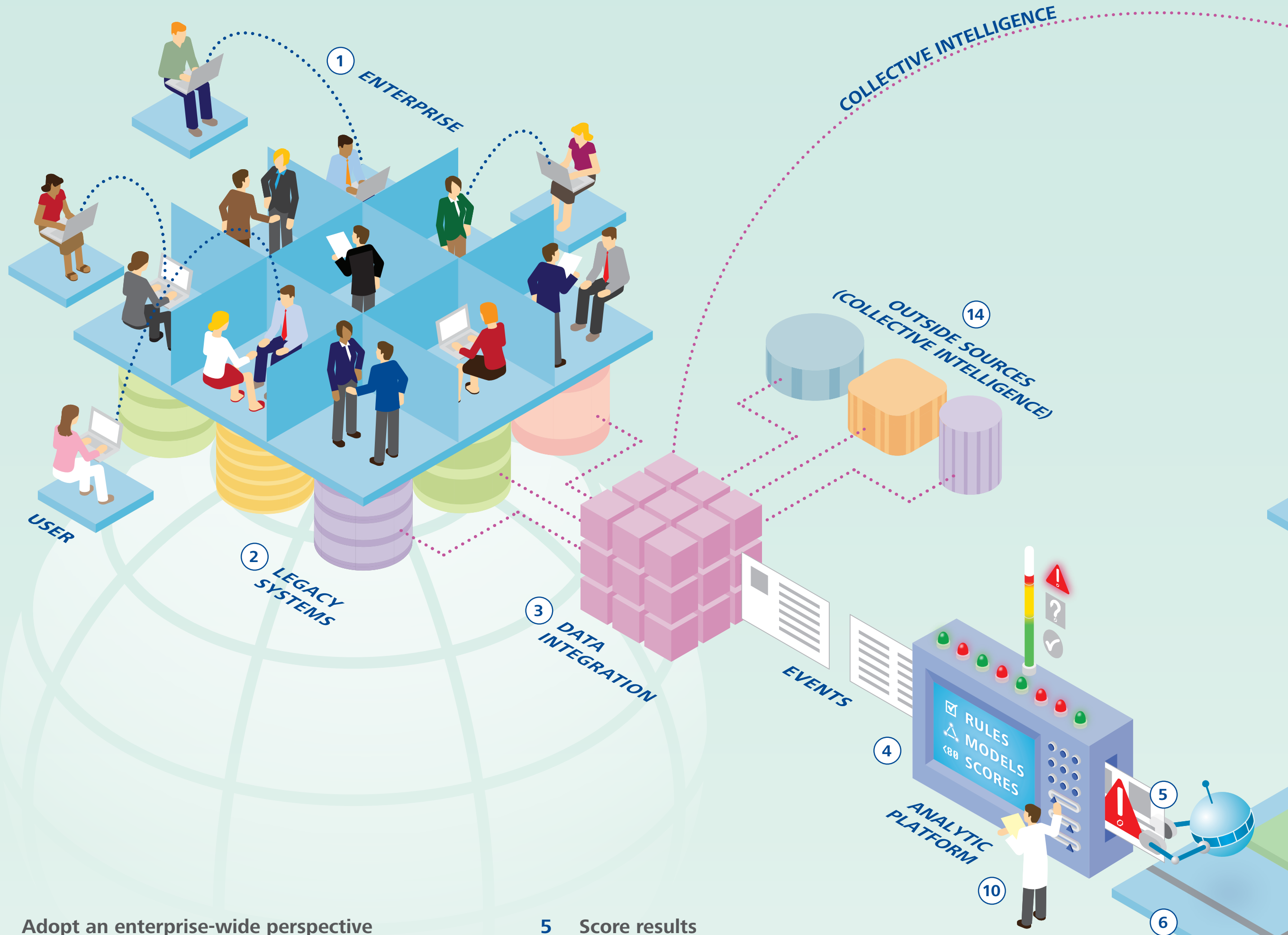
Traditionally, states and federal agencies thus have approached program integrity reactively: pay first, notice an error later (whether fraudulent or not), and then attempt to "chase," or recover, the funds. By doing so, they're missing the low-hanging fruit: the prevention of improper payments in the first place. It's well known among program integrity professionals that prevention is much more cost-effective than after-the-fact recovery.[37]

Prevention identifies and vets cases in which an erroneous payment is likely. A prevention-focused strategy can be doubly lucrative: Prevention saves not just the cost of overpayments, but also the cost of the chase. Potential fraudsters, moreover, are often discouraged from committing fraud and abuse if they know their behavior is being watched.

Prevention, of course, isn't a complete substitute for pay-and-chase. Retrospective strategies such as forensic investigations are an integral part of a comprehensive approach to program integrity, and should be used alongside preventive strategies.

Here's how such an approach would work. All transactions—such as applications or benefits claims—are recorded in a central warehouse. These records power the system's

Figure 3. Flexible and holistic program integrity platform design



1 **Adopt an enterprise-wide perspective**
Take a holistic view of fraud, waste, and abuse risk across the ecosystem of internal and external stakeholders.

2 **Work with legacy systems**
Integrate into existing information systems and technical architectures, without requiring those technologies to be rebuilt or reconfigured.

3 **Integrate data to increase collective intelligence**
Fuse structured and unstructured data streams from internal operations, accounting, and communications systems. Then select third-party data providers and other external claim and non-claim data sources to produce enterprise-view insight into accounts, individuals, and relationships.

4 **Apply the right analytics at the right time**
Dissect and understand transactions and events in near-real time by applying sophisticated business rules and advanced analytics, including cognitive technologies, predictive models to diagnose fraud patterns and profiles, anomaly detection to flag suspicious behavior, and social network analysis to uncover fraud rings, collusion, and kickback schemes.

5 **Score results**
Calculate data-driven fraud risk scores based on the aggregation of all business rules and models to profile transactions, events, and activities to facilitate downstream review, investigation, or intervention as necessary.

6 **Prioritize results**
Route the scored results for each transaction into functional workflow streams. Low-risk transactions are processed in the regular course of business; transactions marked as requiring further investigation are channeled to investigative teams for analysis. High-risk transactions are channeled for various types of countermeasures.

7 **Leverage specialists**
Investigate the prioritized flagged transactions with forensic methods and protocols, resulting in either a recommendation to process the transaction normally or stop it entirely.

8 **Request additional information**
Enrich the investigative results by accessing supplemental and explanatory information from the integrated data repository.

9 Take action
Protect the agency from identified fraud risk and loss with definitive countermeasures, including blocking fraudulent transactions before assets are compromised, intervening via soft notices, initiating formal investigations and providing evidence for criminal prosecution, and closing policy loopholes and implementing front-end edits to mitigate future risk.

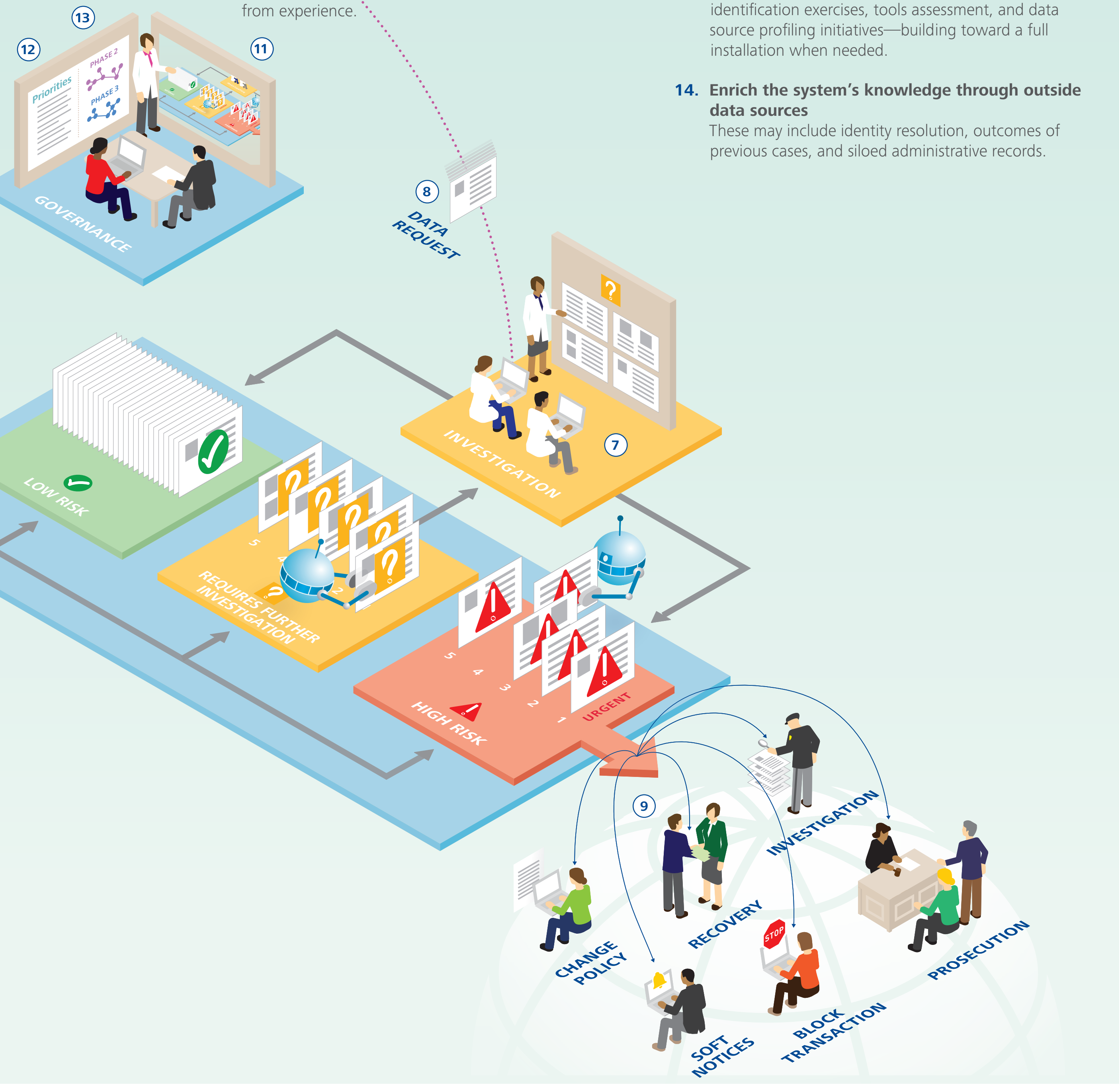
10 Get smarter
Optimize the business rules, advanced analytics, and scoring models over time by factoring in actual results, newly identified risks and updated intelligence, and changes to organizational strategy, policy, and controls. Collective intelligence increases as the system learns from experience.

11 Scale solutions
Calibrate the program integrity solution to the structure, which may involve multiple locations and diverse operations or a single group focused on one department.

12 Tailor solutions
One size does not fit all. Adapt the program integrity solution to the specific organization, strategy, priorities, and risk factors; business segments and product or service lines; and geographies.

13 Build the solution in steps
Design and forge the program integrity solution incrementally, beginning with pilot project efforts, risk identification exercises, tools assessment, and data source profiling initiatives—building toward a full installation when needed.

14. Enrich the system's knowledge through outside data sources
These may include identity resolution, outcomes of previous cases, and siloed administrative records.



"forensic" capability, allowing investigators to look at the record and learn what actions were taken, by whom, and when. When the system notices an erroneous or fraudulent payment has been made, the investigative unit can be called into action to retrieve the funds, as in traditional pay-and-chase.

But the system is also *prospective*, because it creates a knowledge base about prior transactions and outcomes, which allows for predictions about *future* transactions.

Two additional strategies discussed next, behavioral science and collective intelligence, can further enable governments to be proactive in tackling fraud, waste, and abuse. Rather than wait for tips from hotlines, data can identify "hot spots" of waste and fraud and apply behavioral science interventions to prevent them before payments are made.[38]

Use "choice architecture" to encourage compliance

Fraud control efforts are made more difficult by a nonintuitive but important statistical phenomenon called the "false positives paradox." (See sidebar, "The problem of false positives.") When a population produces a low rate of fraud, even a highly accurate fraud detection system will yield a surprisingly high share of false positives.

For this reason, even highly accurate fraud classification algorithms carry a degree of inherent risk. Given the likelihood of false positives, you simply can't automatically accuse a flagged individual.

Advances in statistical modeling, however, can help mitigate the false positives paradox. "Soft-touch" behavioral tactics are particularly well suited to the ambiguous nature of algorithmically generated fraud indications.

THE PROBLEM OF FALSE POSITIVES

Impressive accuracy in a predictive model doesn't always lead to actionable intelligence. To illustrate, consider a hypothetical type of fraud with a 2 percent prevalence—or "base rate"—in the overall population. In other words, about 20 out of each 1,000 cases sampled at random are expected to involve this type of fraud.

Next, suppose a data scientist—call him Dr. Keyes—has built a statistical fraud detection algorithm (or "fraud classifier") that is 95 percent accurate.[39] With this level of accuracy, he would be the envy of his peers. Finally, suppose this algorithm has flagged Mr. Neff as a suspected fraudster. What's the probability that Neff is actually a fraudster? Perhaps surprisingly, the answer is considerably lower than 95 percent.

To understand this, let's return to our hypothetical expectation of 20 fraudsters in a population of 1,000. Keyes's algorithm's 95 percent accuracy rate implies that the model could correctly identify 19 of 20 cases of fraud. But it also implies that the model will flag an expected 49 of the remaining 980 cases as fraudulent (0.05 x 980 = 49). Neff therefore could be either one of the 19 true positives or one of the 49 false positives. Thus the so-called "posterior probability" that Neff is in fact a fraudster is only *28 percent*.

The model does provide useful intelligence: One would sooner investigate Neff than an individual not flagged by the model. But in practical terms, his flagging remains an ambiguous indicator of wrongdoing.

This ambiguity becomes a bigger problem when fraud detection is scaled to larger samples. Consider, for example, California's Medicaid program, Medi-Cal. In 2011, Medi-Cal's fee-for-service program processed 26,472,513 claims.[40] Medi-Cal reported that 4.1 percent (49 of 1,168) of sampled claims were potentially fraudulent in 2011, the latest year for which data were available at the time of publication. Extrapolated to the 26 million claims processed during that quarter, more than 1 million of those claims are likely to show indications of potential fraud.[41] If California had a classifier that could detect fraudulent Medicaid claims with 95 percent accuracy, it would *still* be expected to generate more than 1.2 million false positives.

Relatively easy and inexpensive interventions based on behavioral science can yield significant benefits.

While academics have studied behavioral economics for decades, government agencies only recently have begun using behavioral techniques to reduce fraud, waste, and abuse. Unlike pay-and-chase approaches, behavioral "nudges" are subtle and preventative in nature.

Furthermore, data-driven nudge tactics sidestep the problem of false positives because they don't involve hard accusations or economic penalties. Nudges delivered through carefully worded communications can achieve impressive results at a much lower cost than traditional methods.

Take, for example, the New Mexico Department of Workforce Solutions (NMDWS), which administers the state's unemployment insurance (UI) system. While NMDWS has modernized systems by introducing electronic filing, the department still loses millions of dollars annually to improper payments, mostly due to minor inaccuracies in self-reported beneficiary information.[42] Applicants may overstate how long they've been unemployed or make exaggerated claims about their search for work. NMDWS recently experimented with behavioral economics to reduce such fudged claims.

New Mexico's new UI system identifies the questions to be used in initial applications and ongoing weekly certifications. For each question, NMDWS crafts a "nudge" to encourage beneficiaries to provide the most accurate response. It uses randomized controlled trials, known as A/B testing, to evaluate the economic impacts of each intervention. Because of the size and timeliness of the information gathered, New Mexico officials can observe in near real time the degree to which potential wordings succeed. The process is very similar to the way many private companies use A/B testing to optimize their web pages for sales or views.

NMDWS found that targeted behavioral techniques applied at key moments effectively reduced improper payments. For example, claimants who receive a tailored pop-up message such as "Nine out of 10 people in your county accurately report earnings each week" are nearly twice as likely to self-report earnings. This directly translates to substantially lower improper payments.[43]

> Nudges delivered through carefully worded communications can achieve impressive results at a much lower cost than traditional methods.

Share intelligence to reduce intentional fraud

Handing out government benefits can seem simple; you simply establish that a person qualifies and then deliver his or her payment, grant, or subsidy.

But some systems are more complex. The line connecting a sick patient with Medicaid can pass through doctors, managed care organizations (MCOs), pharmacies, regulators, state governments, and the Centers for Medicare & Medicaid Services. Such complexity translates into greater vulnerability to fraud and abuse.

Tennessee, however, uses *collective intelligence* to extend its investigative reach, so its system can screen for and share instances of fraud, waste, and abuse across the entire network, instead of each being siloed within the organization.

Collective intelligence is the principle powering Google, Wikipedia, and an increasing number of analytical processes in governments and the private sector. It tells us

BEHAVIORAL NUDGES AND PROGRAM INTEGRITY

The emerging science of behavioral economics provides a wellspring of ideas for subtle design changes in choice environments that can "nudge" beneficiaries to interact with benefits program systems more honestly. Health care providers and other third parties, in turn, can be nudged to comply more fully with program requirements.

Similarly, adjudicators can be nudged to rely on more complete, less-biased data when making decisions. Better data and procedures can even nudge auditors to avoid potential cognitive biases in selecting and reviewing cases. Such nudges, in the form of personalized feedback on deviations from expected behavior, outcome evaluation reports against benchmarks, or even a simple checklist of desirable action steps, can be used effectively during the in-line processing portion of an enterprise approach in the prevention of fraud, waste, and abuse.

For a collection of other nudge tactics for benefits program integrity, view the interactive graphic accompanying this study.

that many people working together can be smarter than one or two highly capable people working alone.[44] Collective intelligence takes many forms, from the group decision making of "smart" management teams to the use of machine learning to find patterns in data, such as Google search trends tracking global flu outbreaks.

Dennis Garvey, director of program integrity at TennCare, Tennessee's Medicaid program, established a collective intelligence approach to combat fraud and waste. He didn't want to duplicate the private audits performed by TennCare's MCOs. Instead, he decided to ask them for a simple piece of information: Which health providers were under investigation by each MCO's anti-fraud units? He intended to share the information both with his own team and other MCOs.

The MCOs initially resisted the request. But, Garvey reasoned, if MCOs are contractors, then the government is the customer—and the customer is always right. After Garvey conveyed his expectations to executives from the MCOs, they agreed to his plans.

TennCare's carefully worded contracts required member MCOs to share information. TennCare can respond to a breach of contract by withholding funds or demanding liquidated damages. Pretty soon, Garvey had no trouble with attendance at his transparency meetings.

TennCare moved quickly to make maximal use of the data it gathered from the MCOs. Claims and services data entered into TennCare's system underwent thorough checks to ensure clean information. These detailed records of Medicaid interactions produced a massive trove of data that powers TennCare's collective intelligence capability, giving it a fine-grained map of normal medical behavior within its member population.

Once TennCare had a clearer idea on what was "normal" in its system, Garvey and his colleagues were able to use this knowledge to discover the abnormal. Collective intelligence gave them a sensitive system for flagging deviations from normal care. This knowledge base enables them to spot trends in fraud, share institutional knowledge, notice overpayments, and identify and disseminate best practices to all MCOs. A provider who bills simple drug tests as more expensive blood work, for instance, gets noticed—and, through provider alerts, TennCare warns other MCOs to look out for the same scam. Among other things, TennCare can match suspect enrollees against state records to see if they are actually alive, and notice when a fraudster has used the same ploy with multiple providers.

By letting private entities compete in terms of price but simultaneously pushing them to collaborate on efforts for fraud reduction, Garvey's TennCare achieved more than any single provider or agency could have alone. TennCare dropped 250 providers from the Medicaid network in the effort's first year alone, saving $50 million. "Partnering with the MCOs to reduce fraud was critical to the results," says Garvey.[45]

Most states have haven't used this kind of collective intelligence, in part because they don't wish to play hardball with providers. But, suggests Garvey, just remember that the government is the customer, and enlist the MCOs to collaborate.

COLLECTIVE INTELLIGENCE AS A TOOL TO FIGHT FRAUD

Collective intelligence—what James Surowiecki called "the wisdom of crowds"—represents a way to broaden the sources of information flowing into a fraud reduction system, as well as to improve the dissemination of results from the system. Collective intelligence from external databases or even social media provides an additional source of feedback that can be used to tune models and update the business rules used in enterprise systems to enhance program integrity. Publishing the results of fraud prevention activities outside agency walls can further inform other agencies about bad actors and new fraud patterns.[46]

For a list of current or proposed collective intelligence initiatives in benefits programs, we invite readers to explore our interactive graphic accompanying this study.

A roadmap to increased program integrity

THE following strategies may help governments adopt a more adaptive and effective approach to reducing fraud, waste, and abuse.

1. Set a high-level goal of adopting enterprise-level integrity management, and then work toward it in small steps

GAO's recent survey of fraud prevention programs found that the most successful agencies are those whose leaders demonstrate a commitment to managing fraud risk and ensure this commitment at *all* levels of their organizations.[47] Once the organization as a whole has adopted enterprise fraud management as a goal, it helps to break up that goal into smaller tasks and carry them out one by one.

The theory of "small wins," pioneered by psychologist Karl Weick in a seminal 1984 article, argues that seemingly insurmountable problems are best tackled by breaking them into manageable chunks.[48] SNAP provides a good example of how this approach works. For several decades, SNAP administrators have diligently plugged small vulnerabilities in their program, such as the risk that recipients will "double dip" by receiving benefits from multiple states.[49] While these improvements were relatively minor considered separately, today the SNAP program is widely recognized for its low rates of fraud and abuse. SNAP improper payment rates fell by nearly 50 percent between 2007 and 2014.[50]

2. Don't just buy a point solution—build an enterprise strategy

To defend program integrity successfully, agencies should consider an enterprise approach coordinated among departments, functions, channels, and related programs. With enough contextual data, fraud and waste indicators can be generated and evaluated in real time using advanced analytics, and appropriate interventions applied based on risk scores.[51]

Many current fraud prevention products are one-off solutions. Software alone, however, will not solve the issue. Domain knowledge is key. Agencies should be careful to avoid Band-Aid solutions that target only certain types of fraudsters. A better strategy embeds technology solutions within core operations by assigning risk scores to all transactions and continuously testing the effectiveness of interventions for each type of risk score. New Mexico's UI program shows this technique reduces fraud, waste, and abuse more cost-effectively than other approaches.

3. Make cybersecurity and identity management central to program integrity

Data warehouses for benefits programs are magnets for identity thieves because of the personal information they contain. Recent thefts of taxpayer data from government agencies highlight the financial incentives for hackers.[52] Yet even as governments try to protect themselves against hostile intruders, employees, and citizens alike *still* want their data conveniently available anytime, anywhere.

It's therefore critical to make cybersecurity a central part of strategic planning and operations. Systems that store personal data should, at a minimum, require two-factor authentication (such as a card and password or ID number). Identity management (which ensures that the right people have access to the right parts of the system) should be a core feature of IT platforms for benefits programs. Sensitive data should be encrypted by default.

4. Think about the people in each stage of your program

Benefits programs depend on systems and processes made by and for humans. Even the smartest systems represent a series of human choices. Officials at the New Mexico Department of Workforce Solutions understand this; their experience with nudges shows that thinking about people at each stage of the program and employing human-centric design can result in more effective systems.

5. Choose an "integrator" for your integrity program

Benefits programs with the lowest levels of waste and fraud are those whose players share what could be called an "integrity ecosystem."[53] As agencies attempt to create effective enterprise-wide systems, they must consider who will serve as integrator—the person or entity that convenes stakeholders and balances their interests. It's important to establish as early as possible who will play this role.

Jamie Ralls and Ian Green from Oregon's Secretary of State's Office found themselves serving as integrators when they pushed for the establishment of a task force of fraud investigators from multiple agencies with overlapping jurisdictions. Jointly, their efforts improved information sharing in Oregon and led to the takedown of the Klamath Falls fraud ring.[54] On a national scale, the Centers for Medicare and Medicaid Services serve as integrator for the "Medicaid ecosystem" that ties all 50 states together through direct funding, common standards, technical assistance, and other coordinating actions.

6. Start with waste, abuse, and error

The best available data argue that intentional fraud typically accounts for a third or less of all improper payments; the data also show that reducing waste, abuse, and error in benefits programs usually costs less than chasing fraudsters. Oregon's Secretary of State began with data matching, comparing beneficiary information against lists of dead people, lottery winners, and prisoners to determine vulnerabilities in the eligibility criteria for Medicaid, SNAP, and Temporary Assistance to Needy Families.[55] Clearing away waste and error can reveal the magnitude and location of true fraud more clearly.

7. Use data to inform your choice of interventions

It's time to rethink the way agencies collect, collate, and process data. Technology now permits us to evaluate more data faster. Analytics can transform raw data into a list of key moments amenable to intervention, as with New Mexico's Department of Workforce Solutions. Data on interventions can help agencies evaluate their impact and make necessary adjustments. And collective intelligence can help agencies ensure data quality and consistency at all levels.

The path ahead

THESE approaches to benefits fraud prevention can help government agencies make their anti-fraud dollars work harder and smarter. They can build platforms that combine predictive analytics, behavioral economics, and collective intelligence into a holistic enterprise system, coordinating data from across the enterprise while remaining agile enough to respond to new vulnerabilities.

At present, benefits programs are still locked in an arms race with fraudsters, each evolving in lockstep as the other hurries to keep pace. But as static, rule-based legacy systems give way to adaptive platforms, government benefit transactions will come to more closely resemble credit card payments, with quantifiable vulnerabilities managed through risk profiles and data-centric interventions.

In a companion piece to this study, we provide a **detailed case study of New Mexico's innovative use of behavioral economics to streamline its unemployment insurance program**. We also discuss numerous strategies for reducing fraud, waste, and abuse in government benefits programs with behavioral nudges and collective intelligence, viewable online at our **interactive graphic**.

Endnotes

1. Matt Vespa, “New report lists 601 ways to save $2.6 trillion over five years,” 2015, http://townhall.com/tipsheet/mattvespa/2015/04/03/new-report-lists-601-ways-to-save-26-trillion-over-five-years-n1980578.
2. Bryan Bender, “How do you buy $7 billion of stuff you don’t need?” *Politico*, December 28, 2015, http://www.politico.com/story/2015/12/pentagon-investigation-billions-broken-by-design-216935.
3. US Office of the White House, “Cutting waste,” https://www.whitehouse.gov/economy/reform/cutting-waste.
4. White House, Office of the Press Secretary, “Executive Order 13576—Delivering an efficient, effective, and accountable government,” 2011, https://www.whitehouse.gov/the-press-office/2011/06/13/executive-order-13576-delivering-efficient-effective-and-accountable-gov.
5. Paul C. Light, *The True Size of Government* (Washington, D.C.: Brookings Institution Press, May 1999), p. 90.
6. US President Ronald Reagan, “Remarks at a White House luncheon with the chairman and executive committee of the private sector survey on cost control,” March 10, 1982, https://reaganlibrary.archives.gov/archives/speeches/1982/31082d.htm.
7. US President Herbert Hoover, “Statement to the press,” September 29, 1947, accessed from the Harry Truman Library on January 15, 2016.
8. Stephen Ohlemacher, “GAO: U.S. government gave away $125 billion in questionable benefits last year,” *Associated Press*, March 17, 2015, http://www.huffingtonpost.com/2015/03/17/us-government-improper-payments_n_6883650.html.
9. In FY2015, out of $137 billion in improper payments, $5.1 billion was recovered, or less than 4 percent, according to the Office of Management and Budget: https://paymentaccuracy.gov/content/agency-payment-overpayment-recapture.
10. Interviews with Beryl Davis, Daniel Bertoni, Kay Brown, Carolyn Yocom, Kathleen King, Seto Bagdoyan, James McTigue, Philip McIntyre, James Healy, and Matthew Valenta, Government Accountability Office, January 2016.
11. The term “improper payments” is defined by statute and partially overlaps, but is not synonymous with, related terms such as “waste, fraud, and error,” and ‘fraud, waste, and abuse.” Though the methodology used to measure improper payment rates is not specifically designed to measure fraud, in this study we treat improper payment rates as the best available national proxy for benefits programs.
12. US Public Law 107-300, Improper Payments Information Act of 2002, November 26, 2002, https://www.gpo.gov/fdsys/pkg/PLAW-107publ300/pdf/PLAW-107publ300.pdf.
13. US Centers for Medicare and Medicaid Services, ”Payment Error Rate Measurement (PERM),” https://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicaid-and-CHIP-Compliance/PERM/index.html?redirect=/perm/.
14. Centers for Medicare & Medicaid Services, “Payment Error Rate Measurement Program (PERM) Medicaid error rates,” 2015, https://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicaid-and-CHIP-Compliance/PERM/Downloads/PERM-MEDICAIDERRORRATES201511192015.pdf.
15. Andrew Austin and Jeffrey Stupak, “Mandatory spending since 1962,” US Congressional Research Service, March 18, 2015, http://www.senate.gov/CRSReports/crs-publish.cfm?pid=%270E%2C*P%3C[%3C%23P%20%20%0A.
16. Improper payment amounts capture some, but not all, of fraud, waste, and abuse. Paymentaccuracy.gov, “High error programs,” https://paymentaccuracy.gov/programs/.
17. Institutes of Medicine of the National Academies, *Best care at lower cost: The path to continuously learning health care in America*, p. 13, September 2012, http://www.nationalacademies.org/hmd/Reports/2012/Best-Care-at-Lower-Cost-The-Path-to-Continuously-Learning-Health-Care-in-America.aspx.
18. PaymentAccuracy.gov, “Improper payment amounts (FYs 2004-2013),” https://paymentaccuracy.gov/tabular-view/improper_payments.

19. See the 2013 analysis by Garrett Hatch, "Improper payments and recovery audits: Legislation, implementation, and analysis," US Congressional Research Service, October 18, 2013, https://www.fas.org/sgp/crs/misc/R42878.pdf.

20. Interviews with Davis, Bertoni, Brown, Yocom, King, Bagdoyan, McTigue, McIntyre, Healy, and Valenta, Government Accountability Office, January 2016.

21. It should be noted that many important government benefits programs are not yet reporting their improper payment rates to the Office of Management and Budget. One huge gap is the Temporary Assistance to Needy Families (TANF) program. Improper TANF payments are not currently tracked due to statutory limitations.

22. Oregon Legislative Fiscal Office, *Budget highlights: 2015-2017 legislatively adopted budget*, September 2015, p. 1, https://www.oregonlegislature.gov/lfo/Documents/2015-17%20Budget%20Highlights.pdf.

23. Les Zaitz, "Oregon food stamp fraud ring operated unimpeded for two years as tips piled up," *Oregonian*, July 17, 2014, http://www.oregonlive.com/pacific-northwest-news/index.ssf/2014/07/massive_oregon_food_stamp_frau.html.

24. Tristan Hiegler, "Food stamp fraud: Massive federal, Klamath County operation nabs 30," *Herald and News*, May 9, 2014, http://www.heraldandnews.com/email_blast/food-stamp-fraud-massive-federal-klamath-county-operation-nabs/article_593fd15c-d73b-11e3-8759-001a4bcf887a.html.

25. Zaitz, "Oregon food stamp fraud ring operated unimpeded for two years as tips piled up."

26. Interviews with Karen Johnson, Bruce Lim, Mark Mimnaugh, and Bob Sands, California Department of Health Services, December 8, 2015; see also Will Evans and Christina Jewett, "Teens claim they were used as fake rehab clients," CNN, July 31, 2013, http://www.cnn.com/2013/07/30/health/rehab-racket-siu-cir-part-two/.

27. US House Energy and Commerce Committee hearing, "Examining options to combat health care waste, fraud, and abuse," Testimony of Dan Olson, director of Fraud Prevention, Health Information Designs, LLC, November 28, 2012, https://energycommerce.house.gov/hearings-and-votes/hearings/examining-options-combat-health-care-waste-fraud-and-abuse.

28. Kristin Finklea, *Identity theft: Trends and issues, US Congressional Research Service*, January 16, 2014, p. 1, https://www.fas.org/sgp/crs/misc/R40599.pdf.

29. Dan Ariely, "The mind's grey areas," *Forbes*, June 15, 2010, http://www.forbes.com/2010/06/15/forbes-india-dan-ariely-the-minds-grey-areas-opinions-ideas-10-ariely.html.

30. The Oregon legislature recently allocated $30 million to improve data matching capabilities for program integrity audits, but has not increased its number of program integrity personnel. Source: Deloitte interview with Oregon officials from Secretary of State's Office, December 2015.

31. John Hudak and Grace Wallack, "Sometimes cutting budgets raise [sic] deficits: The curious case of inspectors' general return on investment," Centre for Effective Public Management at Brookings, April 2015, http://www.brookings.edu/~/media/research/files/papers/2015/04/30-inspectors-general-roi-hudak-wallack/cepmhudakwallackoig.pdf.

32. US Department of Health and Human Services, Public Assistance Reporting Information System, "History," http://www.acf.hhs.gov/programs/paris/about/history; Paymentaccuracy.org, "Supplemental Nutrition Assistance Program (SNAP)," https://paymentaccuracy.gov/tracked/supplemental-nutrition-assistance-program-snap-2014.

33. US House Energy and Commerce Committee hearing, "Examining options to combat health care waste, fraud, and abuse," testimony of Dan Olson.

34. US Department of Labor, *Benefit accuracy measurement state data summary: Improper Payment Information Act year 2015*, p. 7, http://www.ows.doleta.gov/unemploy/bam/2015/IPIA_2015_Benefit_Accuracy_Measurement_Annual_Report.pdf.

35. US Department of Agriculture, *Supplemental Nutrition Assistance Program: State activity report fiscal year 2014*, October 2015, p. 2, http://www.fns.usda.gov/sites/default/files/FY14%20State%20Activity%20Report.pdf.

36. California Department of Health Care Services, "2011 Medi-Cal payment error study," http://www.dhcs.ca.gov/formsandpubs/Documents/Legislative%20Reports/2011_MPES.pdf.

37. See for instance US Department of Justice, "Acting deputy attorney general Gary G. Grindler delivers remarks at the National Institute on Health Care Fraud," May 13, 2010,

https://www.justice.gov/opa/speech/acting-deputy-attorney-general-gary-g-grindler-delivers-remarks-national-institute-health.

38. For example, in one state's Medicaid program, anomaly detection showed urgent care centers with unusual prescriber patterns, suggesting possible diversion of prescription drugs. See Deloitte, "Addressing the challenges of the paradigm shift: Pre-payment and managed care analytics," August 10, 2015, https://nampi.net/images/Presentations/Monday/Monday_240PM_Addressing%20the%20challenges%20of%20the%20Paradigm%20Shift_Olson.pdf.

39. The names of characters in this example are borrowed from Paramount's 1944 film noir, *Double Indemnity*, directed by Billy Wilder.

40. California Department of Health Care Services, "2011 Medi-Cal payment error study."

41. California Department of Health Care Services, "California reduces rate of Medi-Cal payment errors and potential fraud for third consecutive term."

42. Improper payments were estimated at $49,324,720. See US Department of Labor, "Unemployment insurance improper payments: New Mexico," http://www.dol.gov/general/maps/nm.

43. Joy Forehand and Michael Greene, "Nudging New Mexico: Kindling compliance among unemployment claimants," *Deloitte Review* 18, January 25, 2016, http://dupress.com/articles/behavior-change-among-unemployment-claimants-behavioral-economics/.

44. There are many definitions of collective intelligence, but few are specific enough to be satisfying. One we feel works well is a basic question posed by the MIT Center for Collective Intelligence: "How can people and computers be connected so that—collectively—they act more intelligently than any person, group, or computer has ever done before?" See MIT Center for Collective Intelligence, http://cci.mit.edu/.

45. Interview with Dennis Garvey, December 10, 2015.

46. US House Energy and Commerce Committee hearing, "Examining options to combat health care waste, fraud, and abuse," testimony of Dan Olson.

47. US Government Accountability Office, "A framework for managing fraud risks in federal programs," July 28, 2015, http://www.gao.gov/products/GAO-15-593SP.

48. Karl Weick, "Small wins: Redefining the scale of social problems," *American Psychologist*, 39(1), January 1984, pp. 40–49.

49. US Department of Health and Human Services, Public Assistance Reporting Information System, "History."

50. Paymentaccuracy.org, "Supplemental Nutrition Assistance Program (SNAP)."

51. See for example Linda Delamaire, Hussein Abdou, and John Pointon, "Credit card fraud detection techniques: A review," *Banks and Bank Systems*, 4(2), 2009, pp. 57–68, https://www.tigurl.org/images/resources/tool/docs/3269.pdf.

52. Lisa Rein, "How the breach of IRS tax returns is part of a much bigger problem facing taxpayers," *Washington Post*, May 29, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/05/29/how-the-breach-of-irs-tax-returns-is-part-of-a-much-bigger-problem-facing-taxpayers/.

53. The idea of an "integrity ecosystem" is loosely based on William Eggers and Anna Muoio's "Solution Ecosystem" framework. According to their analysis, there is an increasing trend of development of a "solution ecosystem" to tackle "complex, dynamic and seemingly intractable social challenges." The characteristics of such an ecosystem are a wide variety of players, an ecosystem integrator, an innovation engine, a portfolio of interventions, and the presence of market incentives. For more information, see William D. Eggers and Anna Muoio, *Wicked opportunities*, Deloitte University Press, April 15, 2015, http://dupress.com/articles/wicked-problems-wicked-opportunities-business-trends/.

54. Interview with Jamie Ralls and Ian Green, December 2015.

55. Oregon Secretary of the State Audit Report, "Public assistance: Improve eligibility procedures and consider approaches of other states," May 2013, http://sos.oregon.gov/audits/Documents/2013-10.pdf.

Acknowledgements

The authors would like to thank the following colleagues from Deloitte Consulting LLP who made contributions to this study. **Sean Hood** provided much of the content for our collection of specific program integrity strategies. **Daniel Ben-Zadok** provided additional context on program integrity issues. **William Carroll**, **David Duden**, **Rachel Frey**, and **John Gahr**, also of Deloitte Consulting LLP, also provided helpful guidance. **Russ Davis**, **Samir Hans**, **Satish Lalchand**, **Rebecca Lady**, **Darin Srivisal**, **Jessica Vesey**, and **Mike Hall** of Deloitte & Touche LLP helped us to better understand the nuances of fraud-fighting efforts across specific government programs. **Vernon Fernandes** of Deloitte Services LP was also helpful.

Karen Johnson, **Mark Mimnaugh**, **Bruce Lim**, and **Bob Sands** from the State of California's Department of Health Care Services generously shared their experiences fighting fraud and waste in the Medi-CAL program. **Dennis Garvey** of TennCare gave us valuable information about the advances Tennessee is making toward reducing Medicaid fraud and waste. **Jamie Ralls** and **Ian Green** of the Oregon Secretary of State's office talked to us about their efforts to improve data matching and collective intelligence to reduce fraud and waste in Oregon's benefit programs. **Beryl Davis**, **Daniel Bertoni**, **Kay Brown**, **Carolyn Yocom**, **Kathleen King**, **Seto Bagdoyan**, **James McTigue, Jr.**, **Philip McIntyre**, **James Healy**, and **Matthew Valenta** of the Government Accountability Office (GAO) kindly talked to us about general trends in improper payments and reducing benefits fraud risk. **Tom Miller** of the US Department of Health and Human Services provided information about the PARIS program.

Finally, we would like to give special recognition to **Pulkit Kapoor** of Deloitte Services LP, who served as lead researcher for this piece, and whose tireless efforts helped to enhance the study's rigor and depth.

Contacts

Brien Lorenze
Advisory principal (state/local)
Deloitte & Touche LLP
blorenze@deloitte.com
+1 571 814 7560

Satish Lalchand
Advisory principal (federal)
Deloitte & Touche LLP
slalchand@deloitte.com
+1 202 220 2738

Dan Olson
Advisory senior manager
Deloitte & Touche LLP
danolson@deloitte.com
+1 312 965 3617

Sundhar Sekhar
Analytics leader, public sector
Deloitte Consulting LLP
ssekhar@deloitte.com
+1 717 651 6240

Rachel Frey
Principal
Deloitte Consulting LLP
rfrey@deloitte.com
+1 916 288 3972

Michael Greene
Senior manager
Deloitte Consulting LLP
migreene@deloitte.com
+1 617 437 3579

Research team

William D. Eggers
Research director, public sector industry
Deloitte Services LP
weggers@deloitte.com
+1 571 882 6585

Peter Viechnicki
Strategic analysis manager
Deloitte Services LP
pviechnicki@deloitte.com
+1 571 858 1862

Deloitte University Press

Follow @DU_Press

Sign up for Deloitte University Press updates at DUPress.com.

About Deloitte University Press

Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Cover art by Kotryna Zukauskaite

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.