PUBLIC SECTOR

Closing the Trillion-Dollar Gap in Public Payments

By Daniel Selikowitz, Christopher Daniel, Yoshihisa Niwa, Brian O'Malley, Scott St Marie, Rose McClintock, Verra Wijaya, Benjamin Desalm, Richard Sargeant, and Mario Gonsalves

ARTICLE DECEMBER 10, 2025 8 MIN READ

Each year, countries spend more than $21 trillion on support payments for their citizens—primarily in the form of pensions, health care, and income support. But our analysis indicates that more than 5% of those payments—and up to 15% in some regions—are lost or misspent due to fraud and error. That amounts to a loss of $1 trillion to $3 trillion in value annually. Today, new solutions are emerging, many of them enabled by technology such as AI and advanced analytics, to

dramatically reduce these problems. Although solutions vary in complexity, many have already proved their effectiveness in private-sector applications for industries such as banking and insurance, and most deliver an extremely high ROI.

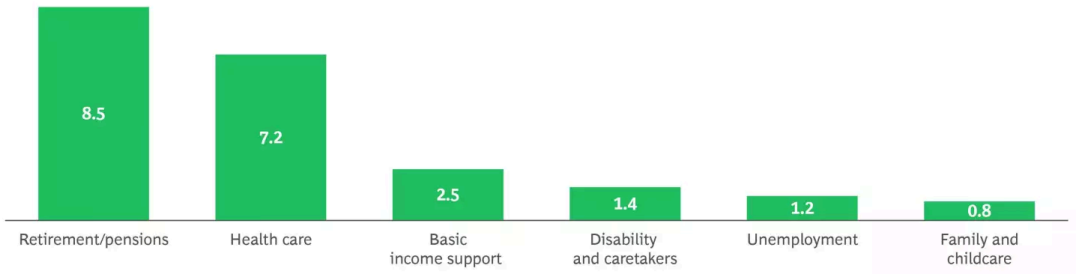
By taking a structured, three-part approach to implementing these solutions—with support from appropriate technology and suitably skilled employees—governments can more effectively reduce fraud and errors and direct the right payment to the right recipient at the right time. In addition to saving a significant amount of money, this approach ensures that countries achieve their intended policy outcomes, and it makes social payment systems more inclusive, building trust among citizens in government overall.

Where and Why Payments Go Wrong

All government payments are susceptible to fraud and noncompliance, but finding a systematic solution to the problem requires understanding where the biggest risks and the biggest opportunities lie. The six biggest categories of support payments are pensions (including social security), health care coverage, supplemental income support, disability and caretaker assistance, unemployment benefits, and family and childcare support. (See the exhibit.) Each of these categories carries different types of risk, including event-based payment triggers and complex, ongoing eligibility requirements.

Governments Worldwide Spent an Estimated $21 Trillion on Support Payments Each Year from 2022 Through 2024

Average annual global government payments by value, 2022–2024 ($trillions)



Sources: International Labor Organization; World Bank; Organization for Economic Cooperation and Development; Office for Budget Responsibility.

Event-based triggers, such as disaster aid, often prioritize speed over comprehensive checks to confirm eligibility—the goal being to deliver funds quickly to people in need. Activity-based payments, such as health care claims submitted after a citizen has received treatment, have a

range of complex characteristics (including eligibility, duration, frequency, modality, and acuity) and are subject to miscoding and overtreatment. When governments make long-term, recurring payments, such as for pensions or public salaries, they face risks such as unreported deaths and duplicate accounts. Periodic payments that involve recurring reviews (for example, unemployment benefits) risk under-reporting and data lags.

Complex conditional eligibility schemes—such as programs for which eligibility depends on a particular medical condition, financial need, or some other means-tested criterion—entail greater risks of fraud and errors. These may take the form of falsified reporting, misdiagnoses, or underreported income. But even simpler categorical eligibility criteria such as age and residence carry integrity risks, such as reliance on outdated registries.

Together, triggers and complex eligibility explain why certain categories of payment, particularly health care and unemployment benefits, are inherently more susceptible to fraud and mistakes. These payments have complex, episodic dynamics and eligibility criteria that change over time, opening more opportunities for fraud and error and creating greater challenges in oversight.

The challenge of fraudulent and erroneous payments is becoming more urgent as a result of fiscal constraints in many countries, aging populations that require more care, increasing health care costs, and other factors. At the same time, fraud tactics are becoming more sophisticated, and the involvement of organized crime increasingly prevalent and decentralized, as bad actors share approaches on social media and use AI to game the system.

As these risks grow more complex, timely action can help governments meet the rising challenge. Thankfully, technology and AI offer new solutions to help them.

Enhancing the Integrity of Support Payment Systems

Bringing greater integrity to government payments requires three principal steps, each of which can benefit from AI enablement and support.

Design Integrity into Systems and Policies

The first and most vital priority for governments is to prevent fraud and noncompliance before it happens. It is much cheaper to halt a fraudulent payment before money goes out the door than to try to claw it back afterward, when audits usually are able to identify and recover only a small fraction of the lost funds. Leaders in the private sector use AI and advanced analytics to identify fraud and errors in real time. Governments can follow suit by designing integrity into their payment programs.

This entails modernizing systems and workflows to include prepayment rules and controls. For example, governments can redesign the interfaces on benefit applications so that they include auto-fill features for key information to reduce errors. The goal is to make compliance easy and noncompliance difficult.

Some organizations have implemented detection models that flag outlier claims and applications and stop or slow noncompliant payments. In the US, some states have introduced predictive analytics to deny noncompliant Medicaid claims, identifying potential savings of up to 1% of total spending—equivalent to nearly $9 billion in annual savings if all states adopted these measures.

Digital verification, another promising design solution, allows agencies to track and reconcile citizen IDs across systems. Agencies can implement secure, digital-first methods for authenticating identity (such as dual-factor authentication with verified credentials) to improve system interoperability and to validate users across different payment schemes in a single operation. Several states in India have adopted biometrically validated citizen IDs linked to digital wallets to enable residents to receive payments. The program has reduced overall per-person spending by 12.7% without any drop in the percentage of households that report receiving benefits, suggesting that some previous recipients may have been obtaining the payments fraudulently.

In some countries, it may make sense for governments to draft new policies and legislation to confer appropriate fraud and noncompliance prevention authority upon specific government entities. Similarly, to eliminate problems with paper payments, governments in some markets may find it advantageous to implement trusted direct payment infrastructure with banks.

Improve Prevention Through Education and Behavioral Nudges

A second crucial lever involves education and deterrence through a combination of accessible information that payees can readily understand and clear messaging about the consequences of noncompliance.

For example, online calculators and self-serve eligibility checks can clear up applicants' misunderstandings. Prompts may flag reviewable errors while the applicant is still entering information, double-checking and requesting additional reviews. AI tools can provide accurate,

easy-to-understand information for applicants and claimants—for example, through the use of AI-enabled smart search and knowledge management tools.

At the same time, education initiatives can reduce fraud and errors by highlighting the consequences of noncompliance. Some governments have run media campaigns to remind people of successful audits. Strategic outreach through forums such as message boards and social media can help agencies meet payees where they are—and where some of them may try to access information about fraud tactics.

Behavioral nudges can also encourage people to adopt proper behavior. For example, the health department in one Asia-Pacific country sent letters to physicians who had prescribed antibiotics at significantly higher-than-average rates. The letters include information about average prescription levels, along with the current prescription rate of the individual recipient. The following year, antibiotic prescription rates among those physicians declined by 12%. These sorts of campaigns can focus on claimants who have been accurately identified as noncompliant or high-risk on the basis of advanced analytics and thoughtful human judgment.

Governments can also build AI-enabled chatbots and contact center tools, such as interactive voice response or next-best-action prompters, to answer the bulk of frequently asked questions about benefits at scale, leading to better outcomes and greater service center efficiency. In Singapore, an AI-powered, natural-language virtual assistant reduced call-center volume by 50% while also reducing inadvertent misclaims and improving service levels.

Be Smarter About Responding to Noncompliant Payouts

The first two measures discussed above are preventive and tend to generate the greatest ROI among payment-integrity programs. In our experience, attempts to recoup a mistaken or fraudulent payment after it has been made often yield only pennies on the dollar. Nevertheless, responding to noncompliant payments is a crucial element of financial restitution, and moreover is vital for deterrence and public confidence in support programs, and many countries can improve their approach in this area.

Again, technology can play a significant role in such efforts. AI can accelerate and automate responses, using behavioral psychology and past campaign results to correctly identify instances of noncompliance and tailor the right approach, thereby alleviating pressure at government agencies that may be understaffed and overwhelmed by employee caseloads. At the same time, it's critical that AI applications have human oversight and judgment to ensure accurate decisions and to avoid false accusations against claimants in cases where no actual issues exist.

Tech-enabled triage can deploy AI to automatically flag potential anomalies—for example, by using machine learning to detect complex fraud patterns and clusters of noncompliance. The

Canada Revenue Agency uses AI-powered risk triage to guide its audit and compliance processes. The agency puts advanced business intelligence tools and algorithms to work analyzing data from sources such as sales tax records, payroll, income tax filings, compliance history, accounting patterns, and unemployment claims. These systems become increasingly accurate over time, through feedback loops that factor in the outcomes of previous investigations to continuously refine detection models.

AI can also assign risk ratings to different payment and claimant types, automatically prioritize predetermined types of noncompliant cases for remediation, and help allocate scarce audit resources where they matter most. In the UK, a data-driven case management platform introduced by the Department for Work and Pensions identifies and rectifies overpayments by integrating data across revenue streams and automatically pinpointing potential overpayments for rectification.

The system assigns different types of resolution mechanisms depending on the degree and likelihood of recovery, ensuring proportional and efficient resolutions that may range from waivers and prospective corrections to claw-backs, deductions, and criminal punishment. By combining automation, analytics, and cross-agency data sharing, the system enables faster detection, targeted interventions, and continuous learning through feedback loops. This approach has reduced future government overpayments by nearly £500 million a year.

AI as a Foundational Element for Success

By adopting the right operating model—one that encompasses a clear vision, organization structure, processes, technology systems, and data—governments can bring together all of these elements. Effective compliance agencies create a culture of accountability so that payment integrity becomes everyone’s responsibility. They put the right authority in place to spur change.

Effective agencies also invest in technology, capitalizing on advances in AI and data analytics to close integrity gaps. Importantly, they recognize—as BCG has through its experience—that technology isn't a plug-and-play fix. Indeed, only about 10% of the value of AI comes from the algorithms, and only 20% from the data. The remaining 70% arises out of revisions to processes, workflows, and employee behaviors. Still, governments that invest in AI with these types of organizational changes—and with the right governance and guardrails—can dramatically improve the performance of their payment systems and generate a sizable ROI.

Implementing advanced analytics may be challenging, but the rewards can be immense. One government agency identified $2 billion in potential savings with a program that used technologies

including AI and analytics to detect payment anomalies. Another is developing a similar program that may yield up to $4 billion in savings on social services payments. These and hundreds of other examples demonstrate a path that governments around the world can take to recoup the $1 trillion to $3 trillion lost each year to fraud and error.

When governments say they can't afford waste, they mean it. And in the end, when it comes to payments, the equation is simple yet profound: reducing fraudulent or mistaken payments makes more funds available, which in turn leads to better public services and greater trust in state capability and fairness. That's an investment well worth making.

Authors

Daniel Selikowitz

Managing Director & Partner
Sydney

Christopher Daniel

Managing Director & Senior Partner; Global Leader, Economic Development & Finance in Public Sector and Center of Government
Dubai

Yoshihisa Niwa

Managing Director & Senior Partner
Tokyo

Brian O'Malley

Managing Director & Partner
Minneapolis

Scott St Marie

Managing Director & Partner
San Diego

Verra Wijaya

Director, Economic Development, Government Finances & Center of Government, BCG Vantage
Singapore

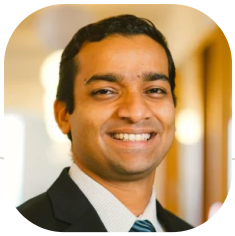
Benjamin Desalm

Managing Director & Partner
Cologne

Richard Sargeant

Managing Director & Partner, Global Leader for City Flow by BCG X, Core Member City Mobility Solutions Hub
London

Mario Gonsalves



India Leader, Public Sector Practice
Bengaluru

ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.