Thomson Reuters Risk & Fraud Solutions:

A new weapon in the fight against fraud, waste, and abuse in government and business

THOMSON REUTERS®

Both the public sector and the private sector are battling an exploding, expensive problem: the billions of dollars lost through fraud, waste, and abuse.

Federal and state governments are always under significant pressure to contain costs and prevent losses, of course. But the recent massive spike of inflation has made this challenge even more pressing. At the same time, incidences of fraud, waste, and abuse have shown no signs of slowing down. This can be largely credited to COVID-19. A recent *New York Times* article reported that government prosecutors are being overwhelmed by the number of cases of fraud involving federal relief programs related to the pandemic, programs that have disbursed trillions of dollars with minimal oversight and regulation.[1]

Fraud is also a critical issue for numerous businesses, particularly (but by no means solely) for financial institutions, mortgage companies, and insurance companies. Companies are fighting an explosion of incidences of money laundering, insurance fraud, mortgage fraud, and cybercrime. The Federal Trade Commission estimates that more than $2.8 billion was lost to corporate fraud in 2021 alone.[2]

If you're a government or business professional involved in fraud investigation, risk management, compliance, or program integrity, you're undoubtedly aware of the problem. What you're seeking are better systems to help prevent, detect, and investigate the rising number of instances of fraud or waste within your systems and programs.

This white paper takes a close look at the challenges of fraud and misspending both in government and in business, many of which overlap. It also introduces Thomson Reuters® Risk & Fraud Solutions, which is comprised of integrated, data-driven solutions that can help customers prevent, detect, and investigate risk and fraud. These solutions have been developed to address multiple complex challenges in both the public and private sectors by combining their expertise with breadth and depth of data, AI-powered analytics, and actionable information. The foundation is Thomson Reuters CLEAR, a public-records database-searching solution that can be used to find information, investigate cases, and detect potential risks. The Thomson Reuters Risk & Fraud Solutions suite is an integrated, data-driven end-to-end solution, and thus can help users prevent, detect, and investigate all sorts of red flags across the entire organization and its processes.

First, let's look at why a toolbox like Thomson Reuters Risk & Fraud Solutions has become so necessary — and has become more and more critical to the operations of both government and business.

The challenge of government fraud

Even before the pandemic and the enacting of legislation to provide financial relief to individuals and businesses, the federal government was paying out trillions of dollars annually through essential programs including (most notably) Medicaid, Medicare, unemployment insurance (UI), the Supplemental Nutrition Assistance Program (SNAP), and the Earned Income Tax Credit (EITC).

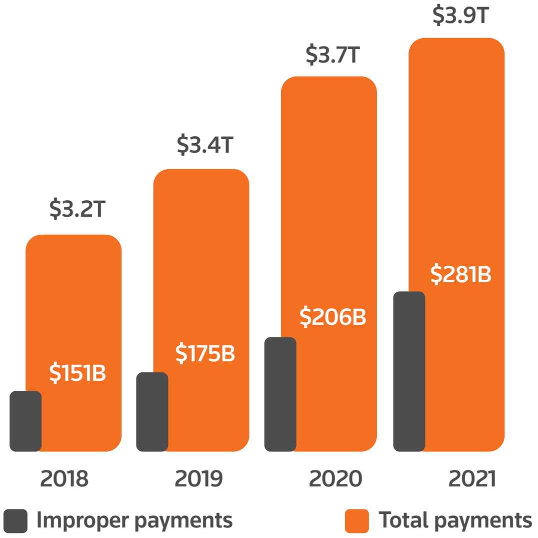
In 2019, the U.S. government distributed an estimated $3.4 trillion via these programs. Of that, about 5% — $175 billion — was determined to be improperly paid. The problem of improper payments only got worse in 2020 when the pandemic hit and governments experienced a massive surge in UI applications. In March 2020 alone, weekly initial claims rose from 211,000 to 6.6 million. The UI program's fiscal 2021 improper payment rate, which was primarily due to fraudulent claims, jumped to 18.7%, roughly 5 to 8 percentage points higher than during the non-pandemic years. The federal Office of Management and Budget has estimated that the UI program has lost at least $163 billion in improper payments during the pandemic period.[3]

With the March 2020 signing of the Coronavirus, Aid, Relief, and Economic Security (CARES) Act and the March 2022 passage of the America Rescue Plan, the government has appropriated around $4.6 trillion in pandemic aid spending. The flood of federal money, combined with the urgent need to deliver these funds, has created the perfect storm for an explosion in fraud and other improper payments.[4]

The chart above shows the steep incline in the federal government's reported improper payment rate over the last four years. Note that the general subsidy outlay has risen from $3.2 trillion to $3.9 trillion. More significantly, the volume of reported improper payments has risen at an even higher rate, increasing from $151 billion in 2018 to $281 billion in 2021. These statistics also show that improper payments were at 5.1% of the total outlay in 2019, rising to 5.6% in 2020, then jumping to 7.2% in 2021. The 2021 total is the highest rate of improper payments since 2003, when the economy began to recover from the recession of the early 2000s.[5] All told, approximately $813 billion has been lost through federal subsidy programs in the last four years.

While the pandemic can partly be blamed for these statistics, they also highlight the limitations of the currently used systems for preventing, detecting, and investigating occurrences of fraud, waste, and abuse. In their investigations, government agencies often have had to rely on outdated internal solutions and information gathered from online searches. The lack of an up-to-date database can severely hamper their investigative work.

Realizing that it needs to address this massive, complex, and costly problem more effectively, the federal government has instituted several programs to better battle fraud and waste:



*Data Sources: **Govwin** and **GAO***

- The federal Center for Medicaid and Medicare Services initiated the Comprehensive Error Rate Testing (CERT) program to measure improper payments in the Medicare fee-for-service (FFS) program starting July 21, 2020.[6]
- The CARES Act instituted a Pandemic Response Accountability Committee (PRAC) charged to prevent and detect mismanagement and misuse of funds while mitigating significant risks impacting numerous government agencies.[7]
- The American Rescue Plan Act of 2021 included $2 billion to support grants towards the prevention and identification of theft and fraud, including the deployment of multi-disciplinary "tiger teams" to work with state UI officials, upgrade outdated IT systems, and propose fraud-prevention strategies.[8]

On November 15, 2021, President Biden signed the $1.2 trillion Infrastructure Investment and Jobs Act, which urged federal agencies "to establish sufficient transparency, accountability reporting, and oversight measures" for specific programs.[9] But unlike the CARES Act, this legislation did not establish independent, coordinated funding oversight. With such a massive outlay of investment underway, it's likely that the government will need to team up with private-sector risk and fraud solutions to provide oversight across these different programs.

The challenge of business fraud

On the private-sector side, the amount of money lost through fraud is just as staggering.

According to Federal Trade Commission data released in February 2022, "American consumers reported losing more than $5.8 billion to fraud in 2021, an increase of more than 70% from 2020." The most commonly reported types of fraud were imposter scams and online shopping scams.[10]

The U.S. insurance industry has been a particular notable victim of fraud. According to the Coalition Against Insurance Fraud, fraudulent insurance claims steal $80 billion annually. These fraudulent activities are carried out in a variety of schemes: padding claims, falsifying facts on an insurance application, staging accidents, and identity theft.[11]

Financial institutions, of course, have long struggled with fraud. According to the UN, money laundering in the U.S. makes up 15% to 38% of the money laundered globally, which is estimated at around $800 billion to $2 trillion. What's more, it's estimated that 90% of money laundering crimes go undetected.[12] By way of comparison, it would take about $6.6 billion a year to eradicate world hunger, according to UN figures.[13] Insurance companies and banks aren't actively fighting to end world hunger, of course, but the comparison is still instructive in highlighting the need for accurate risk and fraud solutions.

And the need extends far beyond the financial services industries. As retailers move further towards online sales, they're being pressed to determine whether customers and vendors are who they say they are — and not cybercriminals looking to steal sensitive company and customer data. Even smaller businesses are being increasingly victimized. According to a Verizon report, 61% of small to medium-sized businesses experienced a cyberattack in 2021.[14] Many attacks didn't succeed, but the statistic does demonstrate that it's not only big companies that have to worry about potentially disastrous data breaches.

Whether the organization seeking to better protect itself is a business or a government agency, the most effective solutions can prevent fraud, waste, and abuse, detect it when it has occurred, and investigate to identify what data sets are fraudulent or out of date. A powerful solution is both preventive and curative. But as governments and businesses look for effective risk and fraud strategies, there are three problems they both typically need to address: accuracy, context, and usability.

The accuracy problem

Data analysis is a complex venture in any industry or government agency, and it's often plagued with accuracy issues, especially when a voluminous amount of data needs to be analyzed rapidly.

Here's a real-life example. In 2018, in a bid to reduce identity theft, Congress passed legislation requiring the federal health care agency in charge to issue health benefit identification cards without Social Security numbers printed on them by April 2019. This required the agency to issue and mail more than 60 million cards within a very short period of time.

At the same time, the program needed to verify recipient addresses. Mailing-address errors can cost the federal government millions in postage and — should the cards fall into the hands of the wrong people — potentially billions in fraud. To ensure that these cards were mailed to the proper recipients, the agency embarked on a systemic data review that compared the information in its pre-existing database against external data sources. The agency invited three private-sector companies to participate in a pilot test of solutions to address this issue. One of those companies was Thomson Reuters, which utilized a version of CLEAR, a core component of Thomson Reuters Risk & Fraud Solutions.[15] Using CLEAR, Thomson Reuters was able to verify all 60 million addresses ahead of schedule by coordinating an effective data-sharing and collaborative process with the agency.

The context problem

This is related to the problem of accuracy. Risk and fraud solutions typically offer impressively high-powered digital technology. But when it comes to generating accurate data analysis, tech isn't always sufficient. Often, data sets are complex, potentially leading to false positives and false negatives. That's why data analysis shouldn't end with the digital review and categorization of data. Data can't be fully understood or analyzed without understanding its context. Relying only on machines can result in problems such as data-driven false positives and negatives.

To illustrate, say a government benefit program is intended only for residents of California. Tech-driven data analysis would likely flag every application originating from outside the state as being fraudulent or improper. However, if the law that establishes such a benefits program allows Californians living and working in other states to apply, there's a risk of cutting off benefits to people legitimately entitled to them.

A good second step would be to sift the data — identifying those who qualify based on this legal proviso. What is lacking between the first step and the second step is context. Thomson Reuters Risk & Fraud Solutions provides this context by adding to its digital capabilities an in-house special investigative unit that comprises data analysis and subject matter experts in the various core benefit programs and markets. These are program or policy experts with decades of experience, and they've often actively investigated instances of public benefits or business fraud. Many also have prosecuted these claims or presented them for administrative, civil, or criminal action. They understand the elements of fraudulent activity, the common scams, and how these activities can manifest themselves in data.

Let's return to the health-benefit card program. During the address verification exercise, decisions had to be made regarding those addresses that landed in the "NO" (that is, unverified) category. Thomson Reuters was able to tap the expertise of its in-house data scientists and analysts to come up with "reason codes" for why these addresses were not verified. These codes were able to provide insight into how to find beneficiaries whose addresses weren't verified via digital analysis.

With its combination of technical developers, proficient data analysts, and subject-matter experts, the Thomson Reuters team have put together a more complete, more accurate solution for detecting fraud, waste, and errors while reducing data-driven mistakes and false positives.

This kind of two-step solution can be deployed by both government and business. For investigations of insurance claims, it can be used to analyze addresses and other relevant data. It could also help investigators and police officers track down criminals involved in money laundering or other fraudulent financial activity. Caseworkers in several U.S. counties are already using risk and fraud solutions from Thomson Reuters to locate parents who were neglecting to pay child support. Other government agencies have been utilizing risk and fraud solutions from Thomson Reuters tools in attempts to track down family members and relatives before having to send a child into foster care.

The usability problem

The user experience of a risk and fraud solution is just as critical as its accuracy. Businesses and governments have enough challenges without having to fumble with clunky software that's difficult to work with. Risk and fraud solutions must offer technology that is intuitive to use and that can generate useful data in an easy-to-understand manner. A lack of usability ranks high as one of the significant factors for the lower-than-expected adoption rates of digital risk and fraud solutions in both government and business.

This is a problem that Thomson Reuters has addressed in crafting Thomson Reuters Risk & Fraud Solutions. These tools have been combined so that they integrate seamlessly with an organization's or agency's workflow. Its design is based on how investigators have used CLEAR and other risk and fraud solutions from Thomson Reuters over the years. The result is a system that makes it easier for the average user to integrate it into both front- and back-end processes. In addition, Thomson Reuters Risk & Fraud Solutions have adopted a scalable data model that enables nontechnical users to configure the system to their organization's requirements.

The benefits of fighting fraud and managing risk

Whether your work is in government or in business, the benefits of an effective, efficient risk and fraud solution are numerous:

- *Financial benefits:* The financial loss that governments and corporations endure due to the growing proliferation of fraud and the clerical errors that can lead to losses significantly highlight the need to adopt additional risk and fraud solutions.
- *Organizational benefits:* To strengthen a business's or government agency's structure and adequately protect and implement its budget, it becomes necessary to cut out every instance of fraud, waste, and abuse.
- *Trust:* Governments require trust from their taxpayers, who need to perceive that their tax dollars are being used wisely. Customers and vendors need to be sure that they can trust companies with which they do business. If a business doesn't aggressively protect itself, the proliferation of fraud and waste can damage that trust.

The size of the U.S. fraud problem for both businesses and government remains massive, and the threats and risks continue to proliferate. Risk and fraud solutions need to be sufficiently robust to confront these costly, complex challenges head on. Any gaps or weaknesses in these solutions increase the risks, putting both government programs and businesses in peril. A comprehensive solution for the entire fraud and risk prevention process can help you address those pain points, whatever your particular risks might be.

Thomson Reuters is not a consumer reporting agency and none of its services or the data contained therein constitute a 'consumer report' as such term is defined in the Federal Fair Credit Reporting Act (FCRA), 15 U.S.C. sec. 1681 et seq. The data provided to you may not be used as a factor in consumer debt collection decisioning, establishing a consumer's eligibility for credit, insurance, employment, government benefits, or housing, or for any other purpose authorized under the FCRA. By accessing one of our services, you agree not to use the service or data for any purpose authorized under the FCRA or in relation to taking an adverse action relating to a consumer application.

For more information, visit tr.com/clear

THOMSON REUTERS®