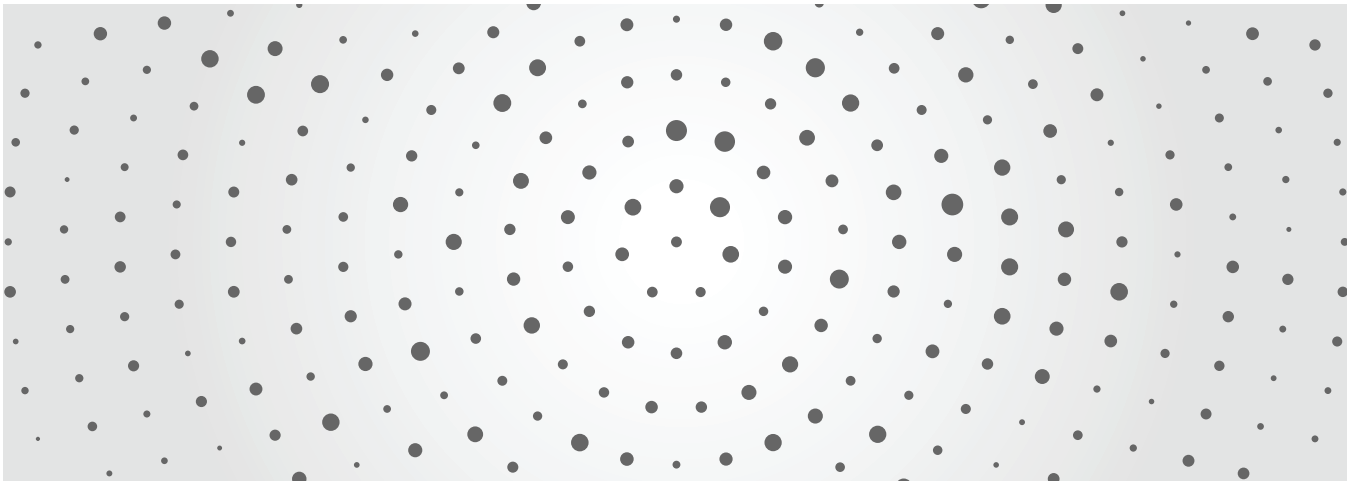
Thomson Reuters Institute

2022 Government Fraud, Waste & Abuse Report

Emerging from the pandemic

THOMSON REUTERS®



2022 Government Fraud, Waste & Abuse Report: Emerging from the pandemic

For the past three years, Thomson Reuters has surveyed state and local government workers to find out how confident they are in their efforts to investigate, detect, and prevent government fraud, waste, and abuse (FWA) — as well as what their steepest job challenges are in terms of resources, staffing, and time.

This report looks at the investigation, detection, and prevention of FWA, as well as the future challenges that state, county, and local governments are facing in addressing this problem and the tools and resources at their disposal for this fight.

Last year's survey happened to coincide with federal efforts to address the COVID-19 pandemic, which heaped enormous pressure on state and local officials to execute federal mandates without much additional staff or monetary support. In addition to managing various business loan and grant programs, state and local governments were responsible for disbursing more than $650 billion in extended unemployment benefits during the pandemic, often while working under stay-at-home orders and other stressful working conditions.

With so much money being distributed so quickly, the danger of fraud was constant. Some fraudsters did successfully exploit weaknesses in the system, of course; but overall, front-line government employees did a remarkable job of maintaining the integrity of their offices and procedures under extraordinarily challenging circumstances.

Study methodology

As the country emerges from the pandemic and the demand for government services returns to levels that are closer to normal, the potential for FWA of government funds still exists, albeit not at the level seen during the pandemic.

This year's study was conducted between March and April of 2022 and included 182 employees from state and local governments around the country. All survey participants work for a government agency or organization and regularly use public records or other risk and fraud solutions as part of their job.

Approximately two-thirds (65%) of survey respondents were government employees at the state level, and the rest were county or city/municipal employees. In contrast to prior years, this year's survey also featured greater participation from investigators, supervisors, and analysts — professionals whose primary job responsibilities involve the use of public records searches and other forms of investigative research.

DEFINING FWA

For the purpose of this report, the phrase *fraud, waste & abuse* is used as a catch-all term for various forms of malfeasance involving government resources. It should be understood, however, that separately, these are three different types of misconduct, not all of which are illegal.

Fraud, of course, is illegal, and generally refers to any effort to deceive the government — through fake documents, stolen identities, rigged contract bidding, etc. — into giving individuals money to which they are not entitled. *Abuse* typically involves a gross misuse of power or resources, and may or may not be illegal, depending on the circumstances. Likewise, *waste* typically involves excessive or unnecessary spending that isn't necessarily illegal.

Even if they are not technically illegal, however, abuse and waste still constitute violations of the public trust, if not the law. Government officials are responsible for protecting public funds against all three forms of misconduct, so for the purposes of this report they are combined, even if the word *fraud* is used independently.

Most common types of FWA

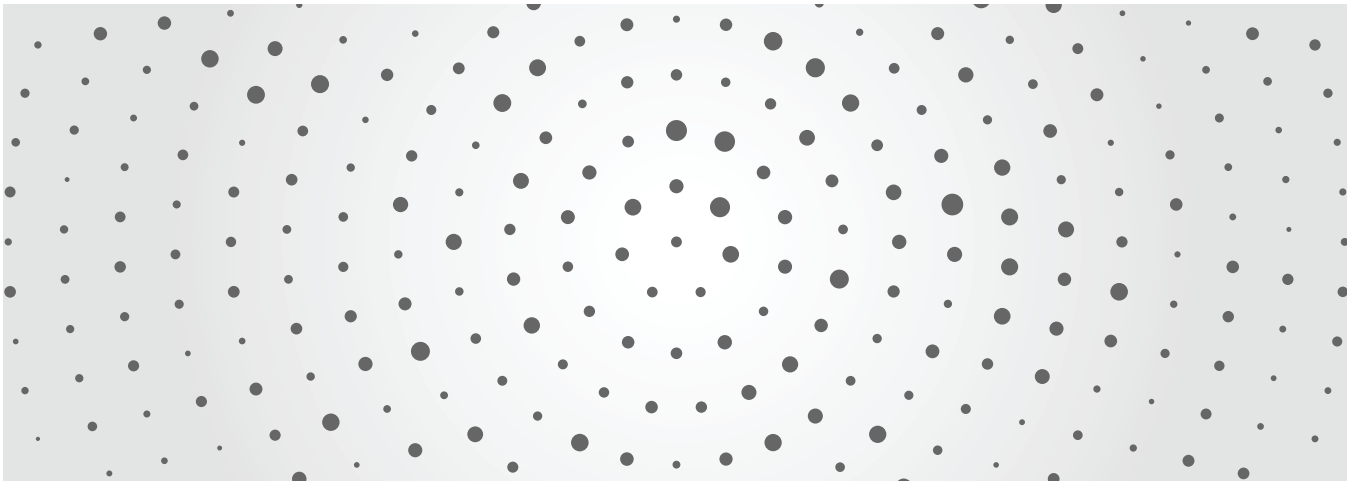
Perpetrators of fraud often target large government programs such as Medicare, federal disaster assistance, and unemployment benefits. During the pandemic, billions of dollars were also stolen from the Small Business Administration's Paycheck Protection Program (PPP) by fraudsters who created fictitious businesses or inflated the employee or revenue numbers of a legitimate business.

In all such cases, people were trying to deceive the government in one way or another; and according to our survey, government employees on the front lines say the most common types of FWA they see are from people submitting false claims and using forged or fake documents to obtain benefits to which they are not entitled.

In terms of frequency, the next-most-common instances of FWA involve billing for unnecessary items or services, charging excessively for items or services, and billing for goods or services that were never delivered, an offense that is often accompanied by falsified records.

Other common types of fraud that government employees are seeing:

- Misusing codes on a claim (*e.g.*, upcoding or unbundling codes);
- Using kickbacks, bribes, or rebates to induce or reward referrals for items or services reimbursed by government programs;
- Unauthorized online access (*e.g.*, account takeovers);
- Synthetic identity or business fraud; and
- Paying for referrals of program beneficiaries.



Prevention, detection & investigation

Preventing, detecting, and investigating FWA are three different facets of the overall effort to protect the integrity of government systems in general. However, each is relevant at different points in the process of applying for, procuring, and disbursing government funds, and each requires a different set of skills and tools for government workers to do the job properly.

For example, *preventing* FWA typically involves systems and procedures at the front end of the process, when vendors and citizens are applying for funds and their identities and other information must be verified. *Detecting* FWA, on the other hand, is largely a matter of monitoring systems for alerts and anomalous or suspicious patterns of activity at almost any point in the process; and *investigating* typically happens after an instance of FWA has been either detected or reported (*e.g.*, from a whistleblower or tip line) — although investigative tools can be employed at any point in the application, procurement, or disbursement process.

Prevention

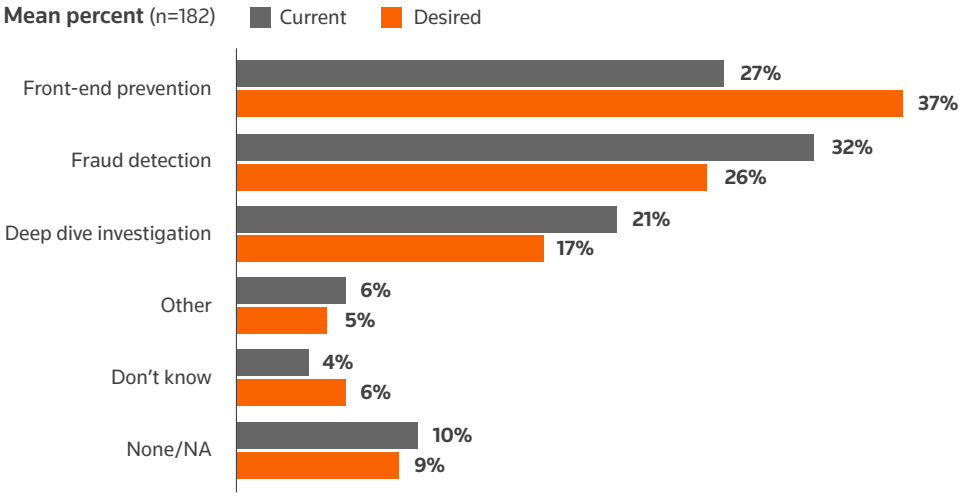
In a perfect system, there would be no FWA, because superior prevention measures would make it impossible, rendering detection and investigation unnecessary. Unfortunately, there is no such thing as a perfect system, which is why efforts to improve current systems and procedures are such a high government priority. And in past surveys, government employees have consistently expressed a desire to spend more time than they already do on preventing FWA from happening in the first place, rather than having to detect or investigate it after the fact.

Consistent with previous results, respondents to this year's survey say they spend an average of 27% of their time on front-end prevention, but expressed a desire to spend as much as 37% of their time on prevention. This desire was even more pronounced at the local level, where respondents say they would prefer to spend more than half (53%) of their time on front-end prevention — up from their current level of 41%.

Conversely, respondents also say they would prefer to spend somewhat *less* time on fraud detection and investigation, an indication perhaps that front-line government employees continue to perceive prevention as a more efficient and effective way to safeguard the public trust.

Figure 1: Focus of fraud, waste and abuse work

In 2022, 27% of fraud, waste and abuse work is focused on front-end prevention, but the desire is to spend 37%.



Q4 What percent of your current fraud, waste and abuse work is focused on each of the following:
Q5 What percent of your fraud, waste and abuse work would your department like to see devoted to each of the following:

Source: Thomson Reuters 2022

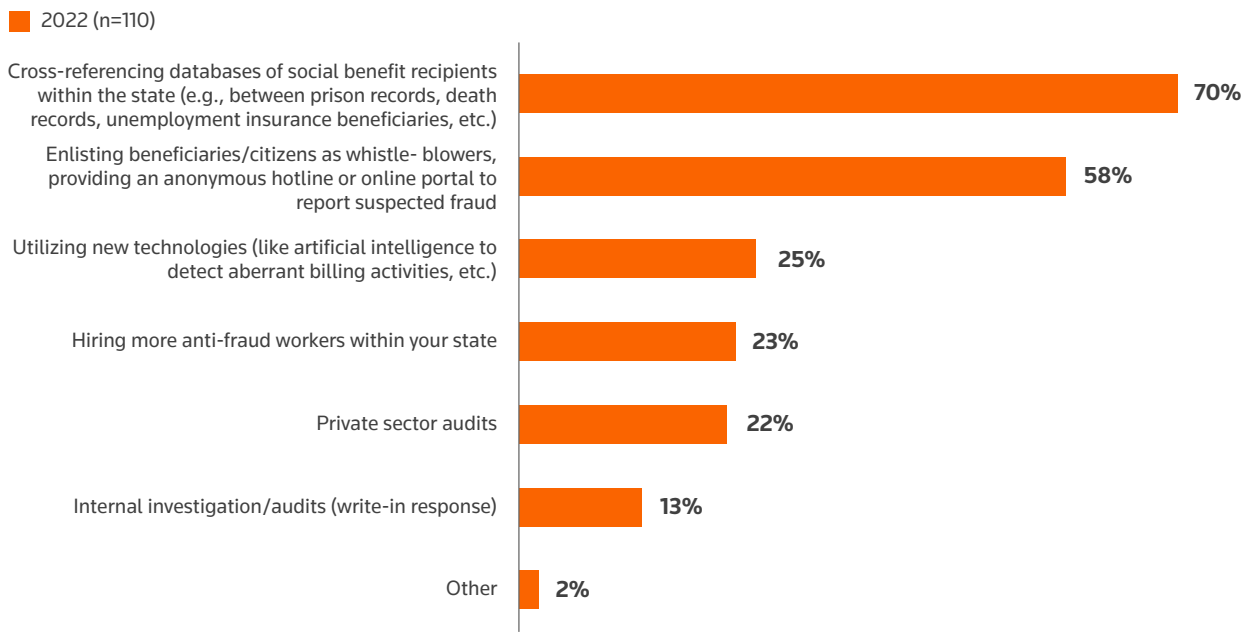
Detection

Whereas preventing FWA involves a great deal of verification, detecting FWA before or as it is happening is often a matter of comparing the right data sets to reveal discrepancies.

Of those government workers surveyed who do fraud detection, 70% say they do so by cross-referencing databases of social benefit recipients within the state — for example, between prison records, death records, unemployment beneficiaries, etc. Further, more than half (58%) say they detect fraud through whistleblowers or citizens calling into tip lines or reporting suspected fraud online, followed by 25% who say they detect fraud using new technologies, such as artificial intelligence capable of identifying aberrant billing activities and other anomalous transaction and behavior patterns.

Figure 2: **Ways in which organization identifies fraud**

70% of those who do fraud detection identify fraud through cross-referencing databases within the state.



Base: Q4 Fraud Detection >0%
Q9 In what ways does your organization identify fraud? Please check all that apply

Source: Thomson Reuters 2022

Another way to detect fraud is by monitoring the current population for changes in benefits eligibility. Of those who perform fraud detection, 47% say their primary source of information is internal department research memos and updates, which often include some sort of communication between an applicant and a government employee. Data from other agencies, states, and benefits programs is the next most common source of eligibility information, and less than one-third of respondents say they get such information through periodic third-party public records reports (30%) or by monitoring social media and negative news (29%).

Investigation

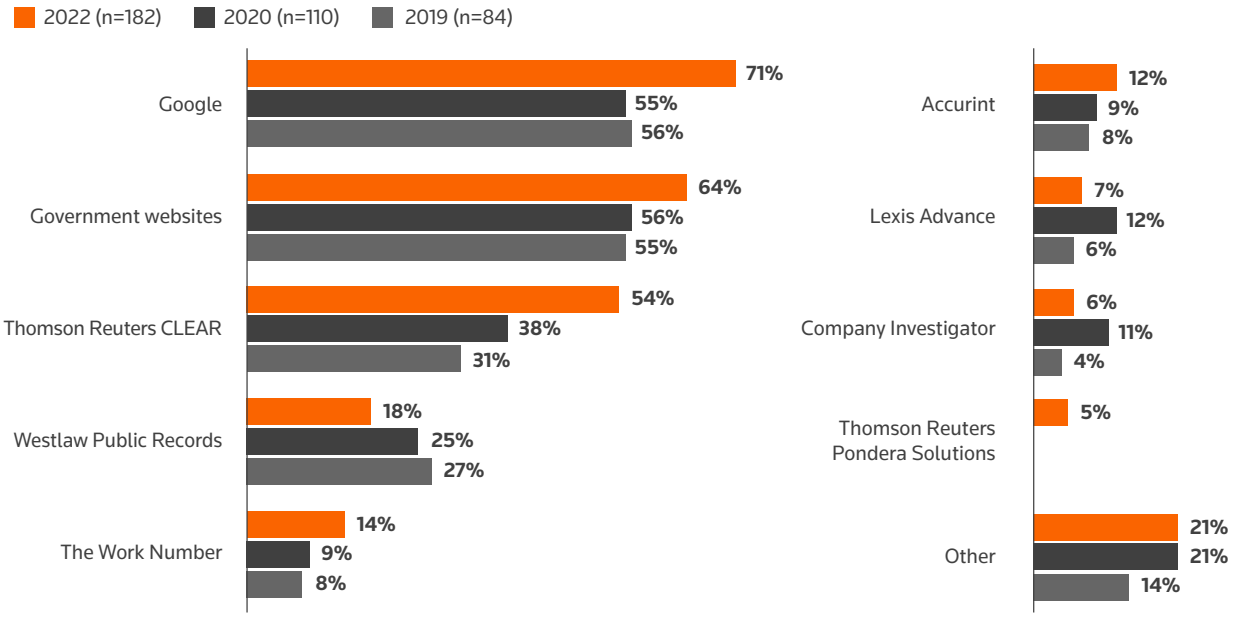
Though investigation of FWA typically happens after suspicious activity has been reported, aspects of the investigation process are involved in prevention and detection as well, primarily by internet searches used to verify information — *e.g.*, identities, addresses, business licenses, employment status, criminal records, etc. — that have been submitted by claimants and vendors.

Not surprisingly, Google is the first stop for many government investigators. Indeed, 71% of government employees surveyed say they use Google to search public records and conduct other investigative activities — and more than half (54%) say they search public records every day.

Although Google is the favorite choice for investigative searches of all kinds, 64% of respondents say they also use government websites, and more than one-half say they use some form of third-party investigative software or a database service, such as Thomson Reuters or LexisNexis, to verify information.

Figure 3: Public records or investigative solutions (top mentions)

Overall, more than 70% use Google for public records or investigations.



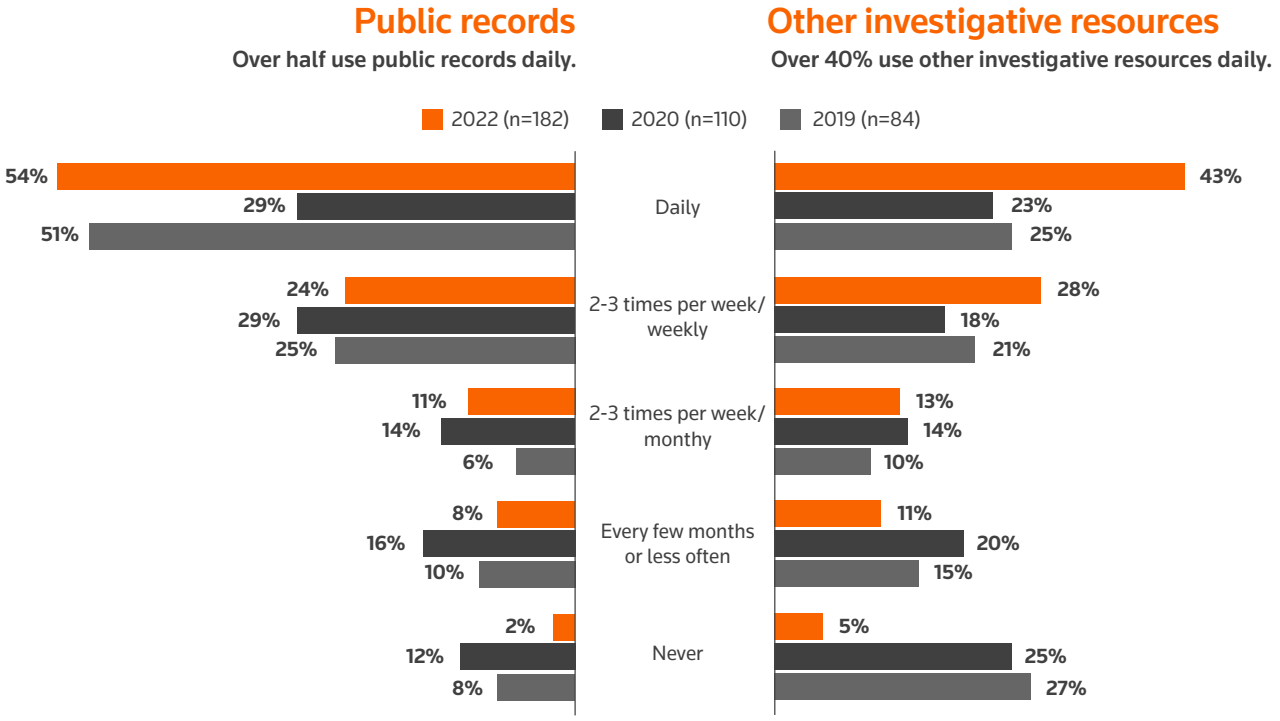
S7 Which of the following public records or investigative products or services do you or someone in your department use? Please check all that apply

Source: Thomson Reuters 2022

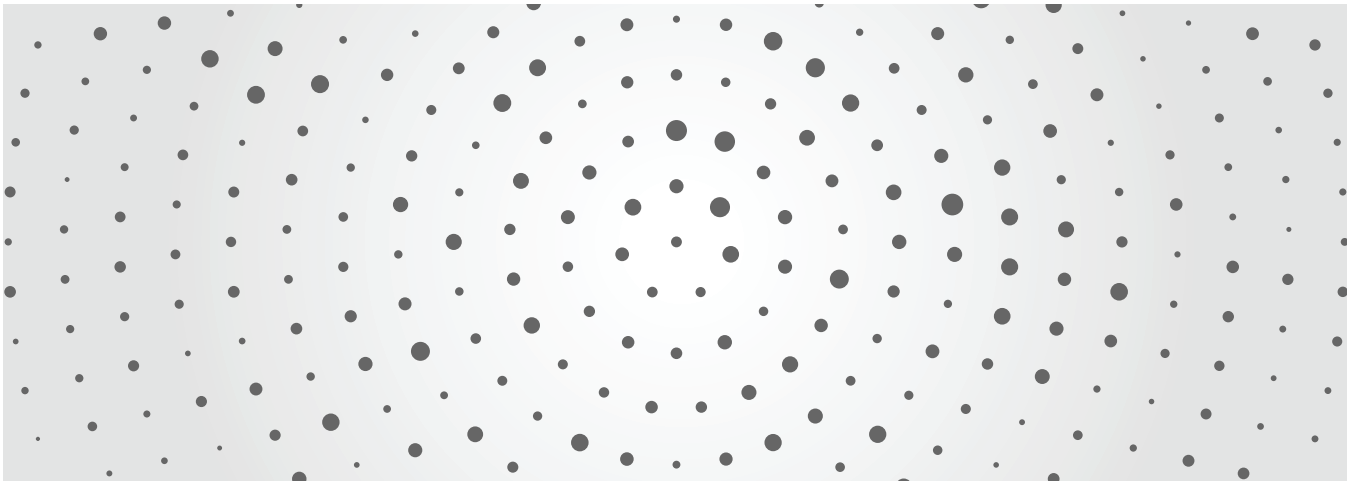
According to the survey, public records on people associated with a business is an investigator's most important information source when performing due diligence, followed by alerts on fraudulent behavior. And among those individuals who conduct fraud investigations, the average weekly number of matters requiring public records searches is 10, two-thirds of which are considered routine.

Yet another indication that government investigators are diversifying their information sources is that 43% of respondents who engage in regular investigative activity say they use investigative resources *other* than public records every day, while 28% say they use alternative investigative resources two to three times per week.

Figure 4: **Frequency of using**



S8 How frequently do you use public records in your job? This could be any public records you access directly or through a service. *Source: Thomson Reuters 2022*



Future challenges

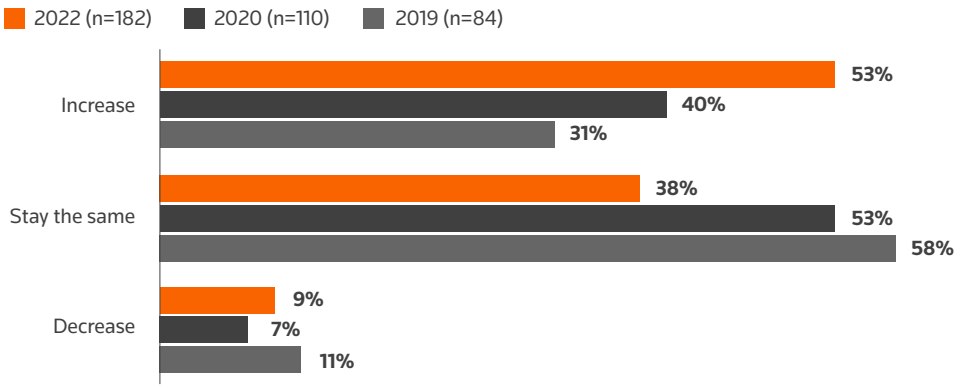
As always, government departments face a number of challenges when it comes to fulfilling their responsibilities; however, over the past two years, the global COVID-19 pandemic has tested the capabilities of state and local governments more than any other event in decades.

Impact of the pandemic

Although the deepest effects of the pandemic have subsided somewhat, about 60% of survey respondents still feel that their fraud prevention, detection, and investigation duties have become more challenging, due in large part to an overall increase in fraudulent activity. Further, more than one-half (53%) of our survey respondents say they expect the prevalence of FWA to increase over the next two years.

Figure 5: **Change in prevalence of fraud, waste and abuse over next 2 years**

In 2022, over half now think the prevalence of fraud, waste and abuse will increase over the next two years.



Q21 Do you think the prevalence of fraud, waste and abuse will increase, decrease, or stay the same over the next 2 years?

Source: Thomson Reuters 2022

About one-in-five survey respondents agreed that the increased sophistication of certain COVID-related fraud schemes exposed unknown systemic vulnerabilities.

One survey respondent notes: "The number of fraud cases has increased significantly, as well as the number of unusual cases. Also, fraud actors adapt and change their claim filing methods to counteract our prevention/detection efforts."

Other new fraud tactics that respondents say they have encountered:

- automated "bot" attacks
- fraud "kits" sold on the Dark Web, with document templates for stolen or synthetic IDs
- multiple e-mail addresses for one e-mail account
- bogus online pharmacies attempting to obtain prescription drugs, and
- multiple social-media schemes using payment platforms such as Venmo, PayPal, etc.

Respondents also cited working remotely and not being able to meet with applicants and vendors in person as contributing factors to making fraud prevention, detection, and investigation more challenging during the pandemic.

Figure 6: Causes of Fraud Prevention, Detection, Investigation Challenges (coded)

The biggest causes of increased fraud in 2022 are lack of in-person activity and more fraud activity in general.

Cause of Increased Challenge (coded)	2022 (n=93)	2020 (n=34)
Lack of in-person activity	34%	32%
More fraud activity	23%	21%
Less access to files / resources (being remote)	18%	24%
Rule changes / new programs	15%	9%
COVID impact / aftermath	12%	–
Less staff	6%	15%
Lack of data / information	3%	–
New vendors / sources of needed goods	1%	6%
Other	10%	9%
NA / None / Don't know	6%	3%

Source: Thomson Reuters 2022

But despite these obstacles, government employees also say they have learned to adapt by using more virtual collaboration and, in some cases, using automated platforms to conduct and complete investigations. More than one-half of respondents also reported that their departments had re-thought the way program integrity duties are performed as a result of the pandemic.

Future departmental challenges

Despite workers' ability to adapt, several ongoing department challenges have remained consistent over the years, many having to do with staffing and budgets. Among those surveyed this year, the top departmental challenges respondents say they continue to face are:

- an increasing volume of work (45%)
- lack of budget or resources (41%)
- recruiting new talent (40%)
- loss of institutional knowledge from retiring staff (37%)
- adoption and implementation of new technologies (37%), and
- keeping up with emerging issues in the field (36%)

At the state level, 37% of respondents cited that staying abreast of the latest investigative techniques and technologies was a major ongoing concern; whereas at the local level, only 17% felt this was an important issue. Also, only 25% of respondents feel that the continuing impact of the pandemic will be a major challenge in 2022, down from 43% in our 2020 survey — yet another sign, perhaps, that the pandemic's impact is indeed receding.

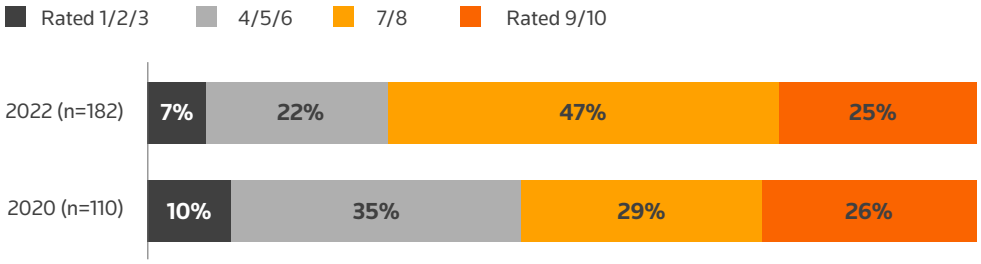
Tools & resources

How effective a government department is at fighting fraud depends somewhat on the tools and resources available to its employees. And in this respect, at least, the data shows some improvement over prior years.

For example, almost two-thirds (63%) of respondents say they felt confident that they have the tools and resources necessary to prevent fraudulent activity — up 13 percentage points since 2020. And almost three-quarters (72%) say they feel confident they have the tools and resources necessary to address investigative issues — up 17 percentage points from 2020.

Figure 7: **Confidence in tools/resources for investigation**

On a scale of 1 to 10, how confident are you that you have the tools/resources to address the investigative issues you face?



Source: Thomson Reuters 2022

True, this year's survey sample included more investigators and supervisors than in the past, so there may be some reluctance to admit to a deficit in departmental capabilities — but these days, any signs of confidence and optimism are refreshing. Indeed, 45% of respondents reported that their departments have allocated at least some of their budget towards tools and resources aimed at fraud prevention — a 10 percentage point increase over 2020, and more in line with responses in 2019.

Figure 8: Percentage of departments that have allocated budget for fraud-prevention tools or resources

Source: Thomson Reuters 2022

Pro-active measures

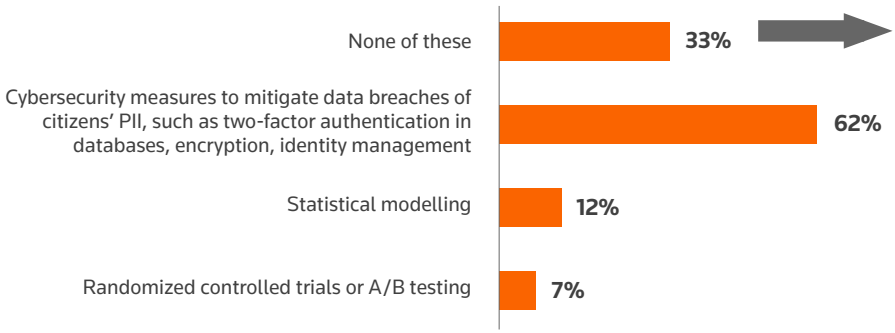
Many (though not all) state and local governments have taken pro-active steps to mitigate the risk of fraud in their programs, primarily by focusing on data security.

Accordingly, 62% of this year's respondents say they have implemented cybersecurity measures to prevent cyber-attacks and data breaches aimed at obtaining private citizen information and other departmental data. These measures typically included two-factor authentication in databases, data encryption, and identity management.

Although it may sound alarming that more than one-third of respondents to this year's survey say they *have not* added extra cybersecurity measures, the reasons why are familiar — primarily, lack of budget and implementation resources, as well as a general lack of technology skills.

Figure 9: Technology tools implemented to mitigate government fraud

Tools implemented in 2022 (n=182)



Reasons for not implementing	2022 (n=60)
Budget	42%
Lack of resources to implement	30%
Lack of technology skills	23%
Other	3%
No Need	10%
None / NA	7%
Don't know	20%

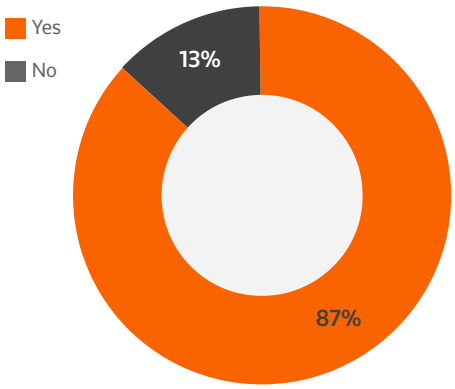
Q33 Which of these technology tools has your organization implemented to mitigate fraud in your government program? Please check all that apply. Base: Q33 = None of these: Q34 For what reasons has your organization not implemented these types of technology tools to mitigate fraud? Please check all that apply.

Source: Thomson Reuters 2022

Further, 57% of this year's survey respondents say they do not track the impact of FWA on their agency, which may contribute to a lack of urgency on the matter. After all, survey-takers note that the most important measure of departmental success in their agency was *efficiency*, followed by public satisfaction with services and the department's case-close rate, all of which could take a hit if, for example, a high degree of efficiency resulted in some FWA slipping through the cracks.

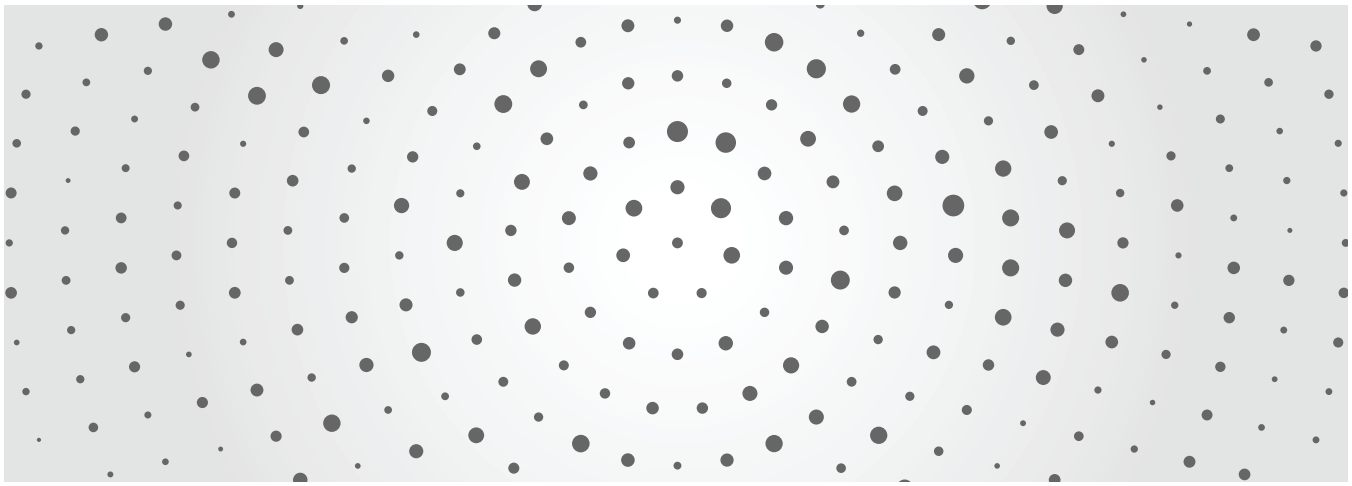
On the bright side, 87% of those surveyed report that they have a process in place whereby a citizen or employee can lodge a fraud, waste or abuse tip or complaint. And as former Assistant US Attorney General Jeffrey Clark noted in a 2021 report from the Department of Justice: "Whistleblowers with insider information are critical to identifying and pursuing new and evolving fraud schemes that might otherwise remain undetected."

Figure 10: **Does your department have a process for lodging whistleblower tips or complaints?**



2022	State (n=118)	Local (n=64)
Yes	92%	77%

Source: Thomson Reuters 2022



Conclusion

As the COVID-19 pandemic recedes into the background of American life, it seems clear that government employees at the state and local levels have weathered the worst and are heading into 2022 with an earned sense of confidence, even though many employees say they expect current levels of FWA to continue or increase over the next couple of years.

As a result of the pandemic, most of the fraud encountered by government employees currently involves submitting false claims and using forged or fake documents to obtain benefits to which these illicit actors are not entitled. However, billing scams and other types of procurement fraud are still prevalent at the state and local level, and fraudsters are still doing a brisk business in forged IDs, business licenses, and other official documents.

However, when it comes to actually preventing, detecting, and investigating FWA, not much has changed over the past couple of years. Google is still everyone's favorite tool for searching public records and verifying information provided by vendors and claimants, but more than one-half of those individuals involved in preventing, detecting, and investigating fraud also use some form of specialized software or a database service to round out their investigative toolkit.

As in previous years, this year's survey reflected a desire among government employees to spend more time on front-end prevention of fraud rather than investigation after the fact. This desire was even more pronounced at the local level, where survey respondents say that if they had their way, they'd spend more than half of their time on front-end prevention — an indication perhaps of the value and effectiveness of proactive risk mitigation.

As in past years too, the major challenges government officials say they expect to face in the near future have to do with an increasing volume of work, lack of budget or resources, difficulty replacing retiring staff, and the struggle to keep up with new technologies and

investigative techniques. These issues are compounded by the expectation that instances of FWA will continue to go up, and the fact that fraudsters continue to search for new ways to exploit systemic vulnerabilities.

Despite these limitations, a majority of those who are actively involved in preventing, detecting, and investigating FWA say they feel confident that they have tools and resources necessary to combat fraudulent activity, and some departments have increased budget allocations for additional resources. Almost two-thirds of this year's respondents also say they have implemented cybersecurity measures, and almost all have some sort of hot line or process for whistleblowers or citizens to leave a tip or lodge a complaint.

Curiously, however, more than one-half of respondents to this year's survey say they do not track the impact of FWA on their agency. It's hard to say, but this oversight may have something to do with the fact that *efficiency* was cited as the most important measure of departmental success, followed by public satisfaction with services and departments' case-close rate — none of which would benefit from reports of FWA that negatively impact the organization.

Thomson Reuters

Thomson Reuters is a leading provider of business information services. Our products include highly specialized information-enabled software and tools for legal, tax, accounting and compliance professionals combined with the world's most global news service – Reuters.

For more information on Thomson Reuters, visit **tr.com** and for the latest world news, **reuters.com**.

Thomson Reuters Institute

The Thomson Reuters Institute brings together people from across the legal, corporate, tax & accounting and government communities to ignite conversation and debate, make sense of the latest events and trends and provide essential guidance on the opportunities and challenges facing their world today. As the dedicated thought leadership arm of Thomson Reuters, our content spans blog commentaries, industry-leading data sets, informed analyses, interviews with industry leaders, videos, podcasts and world-class events that deliver keen insight into a dynamic business landscape.

Visit **thomsonreuters.com/institute** for more details.

THOMSON REUTERS®