Close the gaps to keep employees honest

Quick steps state governments can take to help stop internal fraud

Staggering losses point to massive mitigation opportunity

Unemployment-related overpayments could be at least $163 billion according to a Labor Department top watchdog's recent congressional testimony. As of March 2022, the Labor Department reports the United States has recovered about $4 billion of the wrongful payments.[1] The estimated losses are approximately the combined totals of the entire state annual budgets for Virginia, Michigan, and Arizona[2] and only represent unemployment claims, not other agencies. While the losses are shocking, they spotlight a huge opportunity for states to close gaps that allow fraud, especially when state employees are involved.

External fraudsters who stole billions of dollars in pandemic relief have dominated headlines. Employees have better access, so they steal from the same programs. Based on the current losses, states need proactive and tougher fraud prevention. With the new Department of Justice task force calling for the inspector general to investigate each state for fraud, putting preventative controls in place now can only help. This article introduces a series of steps that allow state agencies to **understand the severity of their fraud problem** and very quickly and cost-effectively **add preventative, detective, and responsive controls to limit employees' opportunities to commit fraud.**

Why modern government is important

Government agencies in the U.S. must modernize in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders of modern governments rethink business processes and service delivery models to more effectively achieve their mission. This article is one of a series that features how modernizing affects the government workforce and the user experience, improves security and public trust, and accelerates the digital journey. KPMG team members offer insights intended to help guide governments in their modernization efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organizations.

[1] Source: Tony Romm, Yeganeh Torbati, "'A magnet for rip-off artists': Fraud siphoned billions from pandemic unemployment benefits," The Washington Post, May 17, 2022.
[2] Source: "List of U.S. state budgets," Wikipedia, May 18, 2022.

Chance lures state employees into crime

New funding sources create tempting opportunities for internal fraud. Agencies received large amounts of federal pandemic funding at a very fast pace that pushed processes to a breaking point. State agencies used to receiving $5 million in program funding annually got $100 million in a year that they needed to disperse to intended recipients in three months. Massive numbers of claims relied on outdated systems unable to handle such a sharp increase in activity.

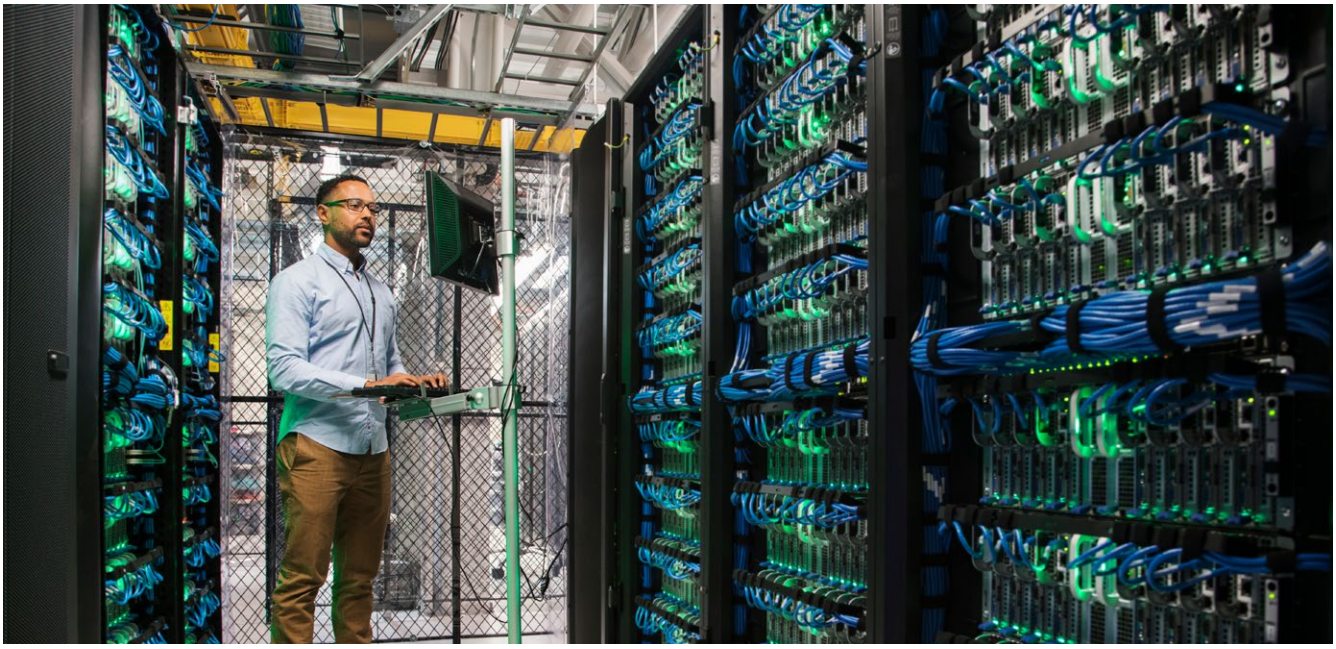
Just in April and the first part of May 2022, the Department of Justice reported guilty pleas, sentencing, or indictments for three separate unemployment insurance fraud incidents involving five former employees in New York[3], Massachusetts[4], and Michigan[5]. In each case, employees stole identities, abused their position and access, and conspired with people outside the agency to submit and approve false claims. One case alone involved $1.6 million in fraudulent payments. With the right controls, these states likely could have avoided these losses.

Synthetic identity theft like this, where fraudsters create new identities with a combination of real and fake information, is the most significant fraud risk for agencies. **Employees have access** to create applicants in state grant management systems and approve payments. Many state agencies do not have efficient or any controls in place to identify false records. As with these cases, employees often collude with family or friends outside the agency to create false records and claims.

Losses also occur outside of pandemic relief. In these cases, **employees have access** to add vendors in state accounts payable systems and ghost employees in human resource systems. In May, the Department of Justice announced a case where authorities arrested and charged two Wayne County, Michigan employees with embezzling over $1.7 million in county funds. The federal government provides the county over $20 million each year to build, repair, and maintain roads. These employees allegedly purchased generators and other equipment from local retailers using taxpayer funds and sold the equipment for personal profit.[6]

Employees such as these know where controls are weak or nonexistent. They know where manual processes still rely on the human eye to see anomalies. Some people abuse their access to information to steal and use or sell personal identifiable information (PII). Even in agencies that use machine learning to spot fraud, some employees are sophisticated enough to know what values to supply the bot to go undetected.

[3] Source: "Former state employee indicted for unemployment insurance fraud," DOJ news release, April 22, 2022.
[4] Source: Joe Silvia, "Former Massachusetts DUA employee sentenced to prison for Covid-19 fraud scheme," New Bedford Guide, April 28, 2022.
[5] Source: B. Thompson, "Former claims manager for Michigan Unemployment Insurance agency pleads guilty in Covid-19 fraud scheme," MIheadlines.com, May 1, 2022.
[6] Source: "Two Wayne County employees arrested and charged with embezzling over $1.7 million in county funds," DOJ news release, May 3, 2022.



Prevention, detection, and response is easier, faster, and cheaper than you might think

Fraudsters will continue to find new and innovative ways to introduce fraud into application-based grant programs. Our approach has evolved to detect such fraudulent applications. It helps minimize overhead cost and time states spend reviewing fictitious applications allowing case managers to focus on payments for nonfraudulent applicants.

Our teams have **implemented anti-fraud AI models with data analytics in state environments in two-to-three weeks** versus months. The iterative approach develops, tests, and deploys fraud detection capabilities using robust modeling techniques to reduce suspicious actors. These include predictive modeling that use natural language processing and computer vision techniques to incorporate actionable patterns and trends extracted from text- and image-based data.

To date, our teams have saved states from paying over $40 million in fraudulent payments across the Emergency Rental Assistance Program (ERAP) program alone. In our recent work with a large state in the northeast, our fraud detection model identified 96.5 percent of fraudulent applications with a precision of 81.4 percent on applications the model predicted to be suspected of fraud.

Monitoring unstructured data is critical to fraud detection

Our experience shows the most significant difference between effective and ineffective controls is the ability to look at **structured as well as unstructured data**. Some states work with fraud mitigation vendors that focus only on structured data that rely on rule-based data models. These standard fraud detection techniques lack the ability to discover trends and patterns that hide from human reviewers. However, using machine learning, advanced models can analyze structured, or form, data and unstructured data that includes PDFs and images to identify potential anomalies and patterns.

Methods that only see structured data miss unstructured data including photo IDs, 1099 or 1040 federal tax forms, income statements, or equipment leases. These data points provide additional details that can help uncover fraud. Details include the time and date a document was created, the document's author, and whether similar information such as signatures and photos have been reused across different applications. Our AI models can review terabytes of data to identify anomalies such as 20 equipment leases with the same signature. Processes that are manual or only see structured data miss what AI models can identify, like fraudulent, digitally altered driver's licenses that lack required information and characters.

Four primary steps

It is **never too late** to take the needed steps **to improve your fraud prevention program**. If your state just received funding and needs to quickly assess for fraud risk based on your current controls, or if you have funding already and suspect suspicious activity, our team can help you develop AI modeling and data analytics that will confirm or deny your suspicion. Not having to worry boosts the return on the investment even more. If there is suspicious activity, we gather information that can be used in an investigation report for the attorney general or inspector general to take the next steps.

1. Assess fraud risk

The first and one of the most important steps to prevent employee fraud incidents like those Michigan, New York, and Massachusetts experienced is to assess fraud risks. The prime time to assess—or re-assess—fraud risk is when your agency is **about to receive a lump sum payment** larger than the agency typically manages. Look closely at how people inside or outside the agency could get away with funds. **Evaluate processes** first and explore preventative measures. **Assess each control**, including manual controls, to see if there are ways around them. Finally, **analyze your technology approach**. Consider adding or expanding AI or machine learning technologies as part of the controls that can keep up with fraudsters' actions.

Spotting trends can help identify control gaps whether your department handles benefit claims, leases, hiring, or purchasing. We take these four main steps to assess fraud risk based on trends:

1. Access the state's intake system, data sources, and existing technology platform.
2. Perform exploratory data analysis with a focus on applications with a final disposition.
3. Segment population into two groups: funding approved and funding denied due to possible fraud.
4. Identify trends and behavior patterns between the two groups based on IP activity, dollar amounts requested, tenant/landlord relationships, and other relevant factors.

Another method with potential long-term value is to **take a holistic look at processes from the outside in**. This helps identify where established processes unrelated to funding administration give employees and their collaborators outside the department access to information they can use to profit. For example, Department of Motor Vehicles accident reports are public record. They include PII such as name, address, date of birth, ethnicity, occupation, and driver's license numbers fraudsters can use to file fake claims. Department of State and other agencies are also possible information sources.

2. Develop an iron-clad fraud policy

Develop a fraud policy and let employees know about the ramifications or action the agency will take if it identifies fraud. The COSO/ACFE Fraud Risk Management Guide provides sample fraud risk management policies as a reference. Based on the sample, a solid policy includes details on these topics[7]:

— Policy statement

— Definition

— Fraud control strategy that includes roles and responsibilities, board and audit committee, management

— Relationship to code of conduct and other company policies

— Fraud risk assessment

— Fraud prevention and detection controls

— Fraud reporting

[7] Source: "CUSO/ACFE Fraud Risk Management Guide," COSO and ACFE, 2016.

3. Educate your employees

Educating employees and managers is a critical part of fraud prevention. Most employees will follow procedures when they understand them and how their actions impact the agency and its customers. Others may follow procedures if they know the consequences. The GAO recommends following these fraud training and education practices to improve fraud detection[8]:

— Require managers and employees to attend training. They should attend training upon hiring and regularly during their employment. For high-risk roles, tailor training to specific jobs.

— Provide training for state employees, contractors, and other stakeholders who play a role in program implementation.

— Tailor fraud-specific information to the program's fraud risk profile.

— Collaborate on training with the Office of Inspector General.

— Promote successful internal investigation results.

— Reinforce anti-fraud messages with employees using other methods besides education.

— Publicize anti-fraud efforts and successfully resolved cases to increase awareness about fraud detection and penalties.

4. Respond consistently

The way an organization responds to and monitors potential fraud defines outcomes. Creating a team that can investigate leads and referrals often get the best results. The COSO/ACFE Fraud Risk Management Guide includes recommended fraud investigation and response protocols agencies should follow to investigate potential fraud.[9] The protocols are based on the principle 4 of a Fraud Risk Management Program: The Guide establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

— Establish fraud investigation and response protocols that support open communication.

— Conduct objective investigations based on the scope and severity of each incident.

— Communicate investigation results to internal and external (when necessary) authorities.

— Take corrective action based on the findings, including asset recovery, discipline, and remediation. This step should also include analyzing internal controls to reduce risks of similar incidents and training on new procedures.

— Evaluate investigation performance based on time and cost to resolve, repeated incidents, locations, value of losses, and corrective actions.

Addressing internal fraud can return more than it costs

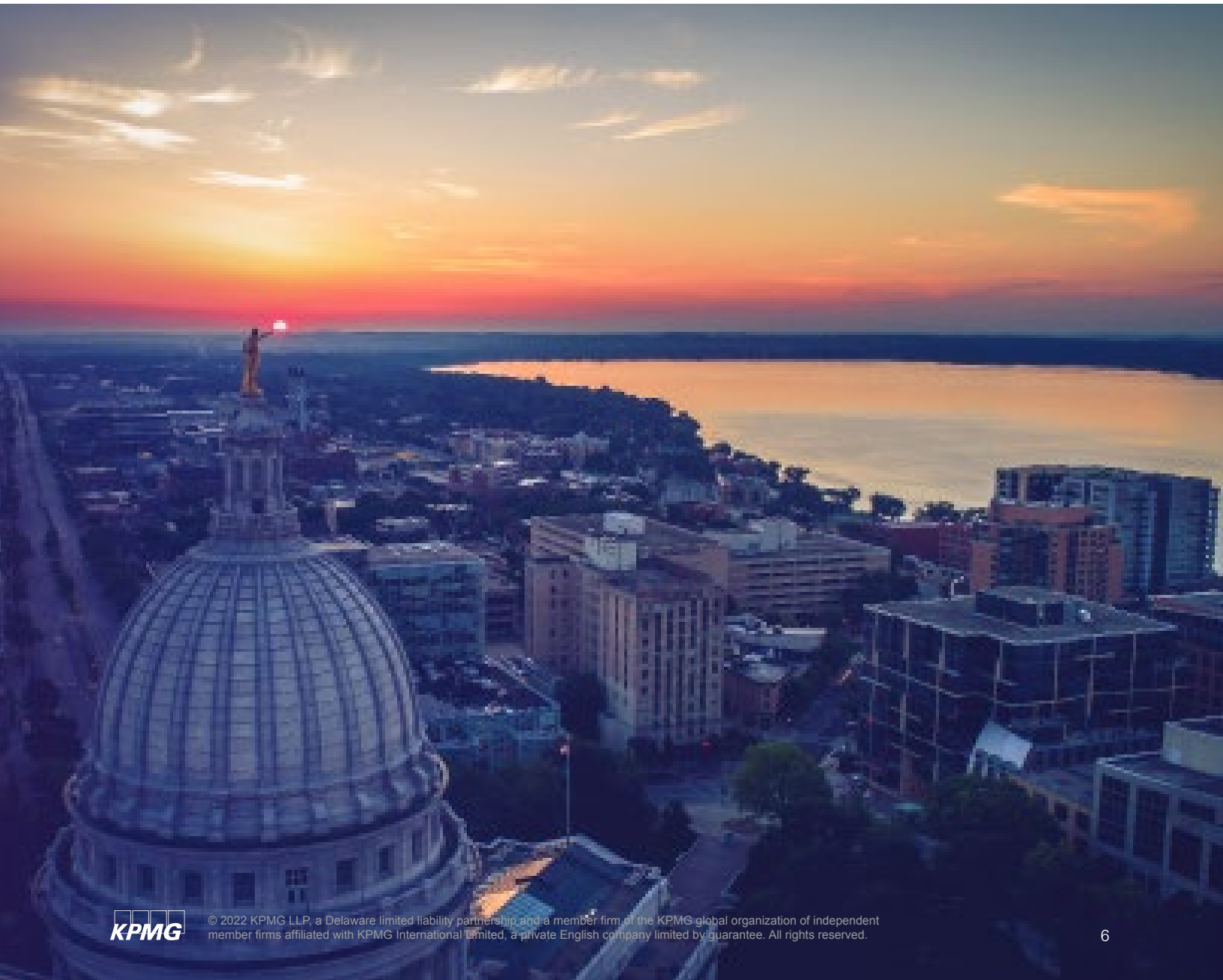
Our teams have implemented anti-fraud models in state environments in two-to-three weeks. The return these states received on their roughly $200,000 investment can return millions in potential fraud identification. No matter where your state is in the process, we can help improve your fraud prevention program. Employees are looking for gaps as you read. Don't allow them to find any.

[8] Source: "A Framework for Managing Fraud Risks in Federal Programs," pages 43-44, GAO-15-593SP, GAO, July 2015.
[9] Source: "COSO/ACFE Fraud Risk Management Guide," COSO and the ACFE, 2016.

About KPMG

KPMG has worked with federal, state, and local governments for more than a century, so we know how agencies work. Our team understands the unique issues, pressures, and challenges you encounter in the journey to modernize. We draw on our government operations knowledge to offer methodologies tailored to help you overcome these challenges and work with you from beginning to end to deliver the results that matter.

The KPMG team starts with the business issue before we determine the solution because we understand the ultimate mission. When the way people work changes, our team brings the leading training practices to make sure your employees have the right knowledge and skills. We also help your people get value out of technology while also assisting with cloud, advanced analytics, intelligent automation, and cybersecurity. Our passion is to create value, inspire trust, and help government clients deliver better experiences to workers, citizens, and communities.



Contact Us

Tom Stanton
Advisory Managing Director,
Forensic
KPMG LLP
212-872-7758
tstanton@kpmg.com

Andrew Neville
Senior Manager, Tax
Economic & Valuation Services
KPMG LLP
703-286-2913
aneville@kpmg.com

Bobby Gorantla
Director, Data Engineer Lighthouse
KPMG LLP
484-319-7937
bgorantla@kpmg.com

---

read.kpmg.us/modgov

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.