Optum Serve®

Reimagining fraud prevention

Modernization for emergency relief programs and beyond

Government pandemic relief programs provided an emergency lifeline to countless residents and businesses. The Coronavirus Aid, Relief, and Economic Security (CARES) Act and others supported paycheck protection, education initiatives, provision of health care and much more. However, in order to deliver payments at the scope, scale and speed with which they needed to reach citizens, the programs were challenged to enact sufficient controls. Perhaps most notably, applicants encountered limited to no prior authorization to verify their identities and credentials before they received the money, making the relief processes highly susceptible to fraud.

As a result, agencies swiftly provided millions of people necessary assistance, but simultaneously lost billions of dollars to fraudulent activity.

"The pandemic really exacerbated the fraud world. Especially looking at the federal programs that were created in such an emergent way, it was impossible with existing agency resources and systems to put the necessary controls in place in such a short amount of time," says Amanda Warfield, vice president of program integrity at Optum Serve, the federal services arm of Optum and UnitedHealth Group. "The pandemic just really created vulnerabilities at levels historically not seen before."

Individuals and businesses took advantage of assistance programs by falsifying information, carrying out identity theft, using funds for extravagant purchases, or even going so far as to create fake shell companies to house illegally obtained payments. Some organized into groups to defraud programs. In the years since, federal entities like the Small Business Administration (SBA), the Department of Justice (DOJ), and all the agency Offices of the Inspector General (OIG) have worked to uncover fraud, bring criminals to trial and restore lost funds.

The CARES Act also established an independent Special Inspector General for Pandemic Recovery (SIGPR). The organization, led by Brian D. Miller, is responsible for coordinating audits and investigations related to tax dollars appropriated by Congress through the CARES Act.

"There's so much fraud going on, it's difficult to catch all of it. Many of these fraudsters have moved on, they've sold their business, converted the money into crypto which is hard to trace," says Miller. "Financial fraud is complex. My office and other offices need the manpower to actually do the legwork and prove these cases, and work with the Department of Justice to bring these criminals to conviction."

"**The pandemic really exacerbated the fraud world.** Especially looking at the federal programs that were created in such an emergent way, it was impossible with existing agency resources and systems to put the necessary controls in place in such a short amount of time."

– Amanda Warfield,
Vice President, Program Integrity,
Optum Serve

"**There's so much fraud going on, it's difficult to catch all of it.** Many of these fraudsters have moved on, they've sold their business, converted the money into crypto which is hard to trace."

– Brian D. Miller
Special Inspector General for
Pandemic Recovery

To provide agencies the resources necessary to build prosecutable fraud cases, the Biden Administration released the Pandemic Anti-Fraud Proposal. The plan announces an increase in the statute of limitations for pandemic-related fraud cases from 5 years up to 10, giving agencies a better chance of catching fraudsters.

Moreover, the proposal calls for agencies to modernize their systems and processes to "learn lessons from what went wrong with certain emergency programs that were subject to significant fraud in 2020 and invest in better prevention of identity theft and all forms of major fraud involving public benefit programs."

Despite federal support, however, the residual impact of COVID-19 fraud will be long-lasting. It will take years for agencies and local organizations to fully recover, prosecute all cases and determine methods to get their money back. Agencies must choose the right practices and partners on the road to modernization to effectively combat past, present and future fraud.

Modernizing programs is imperative for fraud prevention

Disparate legacy systems and outdated processes make it easier for criminals to discover and target vulnerabilities, especially during emergencies. As they rebuild and recuperate, agencies will need to prioritize modernizing their infrastructure to prepare for and prevent fraud in the future.

"We like to see more controls in place, more checks in place, more ways to verify the information that's given by recipients to get the grant, loan or money from the program," Miller says. "It may mean that the money doesn't get out as quickly, but we think it's worth it because otherwise it will be lost to domestic or foreign criminals."

Cross-sector collaboration plays a pivotal role in modernization, Warfield adds. The private sector has a breadth of tools and resources that the government may not otherwise access. With more advanced capabilities, agencies can bolster IT systems and platforms used to manage programs to build in checks and balances from the start.

"On the private side, we can help really put things in place so that when you have to spin up a program quickly, and get emergency funds out the door, you make sure you've got the best tools available that'll help prevent widespread fraud from happening," she says.

One of the main reasons identity theft was so prevalent in pandemic relief programs was agencies' lack of ability to verify application information. Private-sector capabilities could help streamline information sharing across agencies. If organizations are able to quickly and easily communicate and share data, they can immediately verify whether citizen or business qualifications are correct, impeding fraudsters from successfully submitting falsified information.

"That information sharing piece is really huge," Warfield notes. "Some of the loans that went out the door went to individuals who provided fake Social Security numbers. Data sharing across agencies could have prevented some of that from happening."

The federal government has established a number of necessary restrictions to prevent cyberattackers from accessing sensitive data, but this often creates hurdles to information sharing.

Up to 10 years

Statute of limitations increase for pandemic-related fraud cases announced by the Pandemic Anti-Fraud Proposal, giving agencies a better chance of catching fraudsters.

> "We like to see … more ways to verify the information that's given by recipients. **It may mean that the money doesn't get out as quickly, but we think it's worth it because otherwise it will be lost to domestic or foreign criminals.**"
>
> – Brian D. Miller
> Special Inspector General for Pandemic Recovery

Warfield says there are many data-protection methods commonly used in the private sector that would benefit the government. Data masking, or data obfuscation, for example, creates a structurally similar but inauthentic reproduction of an organization's sensitive data that is useless to cyber criminals, but still usable to authorized software and personnel.

"You don't have to physically move the data, but you can still share mass data in a way that might make it easier to get critical inter-agency data sharing agreements in place; those agreements have historically prevented effective data sharing across agencies," Warfield says.

Data masking is just one of many practices that the public sector can implement to share data and information in a more secure way, mitigating the risks to data in transit.

"I think the private sector could be very helpful here – [it has] expertise in data sharing, storing data, clearing duplicates and that sort of thing, in deconfliction with various offices," says Miller. "So there are big ways in which you can make it easier to share, use and keep information to make sure it is accurate."

Invest in the right private-sector partnerships

As an industry partner, Optum Serve is able to leverage the extensive technology and best practices from the enterprise side of its organization to meet the unique needs and requirements of the agencies it works with, including Centers for Medicare and Medicaid Services, Department of Veterans Affairs, Health Resources and Service Administration, and Federal Bureau of Investigation, among others.

Optum Serve gives its government partners better visibility and insight into the integrity of various programs through technology platforms that use advanced analytics and intelligence tools to detect fraud, waste and abuse – both after the fact and proactively. Its integrated data capabilities are also crucial in its work to improve information sharing, introduce automation for document approval and eligibility determination, and build preventive measures into programs.

Additionally, Optum Serve employs a team of investigators and certified coders who take steps to identify, validate and prove a particular fraud claim or allegation, helping propel cases forward to prosecution.

"We specialize in the development and creation of those types of reports and features that enable the government to get what [it needs] quickly to prosecute a case," Warfield explains. "In addition, we also do all of the fraud, waste and abuse oversight for our clients. We do both the IT work to enable detection of leads, potential fraud, unusual aberrant behaviors, and holistic predictive analytics looking for trends."

Moving forward, Optum Serve hopes to continue collaborating closely with public-sector counterparts to pinpoint central fraud challenges and leverage their workflows and resources to create viable solutions for the public sector in the future. This shared goal will help the nation both recover from pandemic fraud and bolster programs without slowing down the public's access to the funds it needs.

Data masking

One of many practices that the public sector can implement to share data and information in a more secure way, mitigating the risks to data in transit.

Optum Serve employs a team of investigators and certified coders who take steps to identify validate, and prove a particular fraud claim or allegation, helping propel cases forward to prosecution.

To learn more about how Optum Serve can help your organization combat fraud, visit:

optum.com/program-integrity-services

Optum Serve®