INVESTIGATING PANDEMIC FRAUD: PREVENTING HISTORY FROM REPEATING ITSELF

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT

OF THE

COMMITTEE ON WAYS AND MEANS

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

OCTOBER 19, 2023

Serial No. 118–OS03

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PUBLISHING OFFICE

54–909 WASHINGTON : 2024

COMMITTEE ON WAYS AND MEANS

JASON SMITH, Missouri, *Chairman*

VERN BUCHANAN, Florida
ADRIAN SMITH, Nebraska
MIKE KELLY, Pennsylvania
DAVID SCHWEIKERT, Arizona
DARIN LAHOOD, Illinois
BRAD WENSTRUP, Ohio
JODEY ARRINGTON, Texas
DREW FERGUSON, Georgia
RON ESTES, Kansas
LLOYD SMUCKER, Pennsylvania
KEVIN HERN, Oklahoma
CAROL MILLER, West Virginia
GREG MURPHY, North Carolina
DAVID KUSTOFF, Tennessee
BRIAN FITZPATRICK, Pennsylvania
GREG STEUBE, Florida
CLAUDIA TENNEY, New York
MICHELLE FISCHBACH, Minnesota
BLAKE MOORE, Utah
MICHELLE STEEL, California
BETH VAN DUYNE, Texas
RANDY FEENSTRA, Iowa
NICOLE MALLIOTAKIS, New York
MIKE CAREY, Ohio

RICHARD E. NEAL, Massachusetts
LLOYD DOGGETT, Texas
MIKE THOMPSON, California
JOHN B. LARSON, Connecticut
EARL BLUMENAUER, Oregon
BILL PASCRELL, JR., New Jersey
DANNY DAVIS, Illinois
LINDA SANCHEZ, California
BRIAN HIGGINS, New York
TERRI SEWELL, Alabama
SUZAN DELBENE, Washington
JUDY CHU, California
GWEN MOORE, Wisconsin
DAN KILDEE, Michigan
DON BEYER, Virginia
DWIGHT EVANS, Pennsylvania
BRAD SCHNEIDER, Illinois
JIMMY PANETTA, California

MARK ROMAN, *Staff Director*
BRANDON CASEY, *Minority Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT

DAVID SCHWEIKERT, Arizona, *Chairman*

BRIAN FITZPATRICK, Pennsylvania
GREG STEUBE, Florida
CLAUDIA TENNEY, New York
MICHELLE FISCHBACH, Minnesota
BETH VAN DUYNE, Texas
RANDY FEENSTRA, Iowa
NICOLE MALLIOTAKIS, New York

BILL PASCRELL, New Jersey
JUDY CHU, California
BRAD SCHNEIDER, Illinois
SUZAN DELBENE, Washington
GWEN MOORE, Wisconsin

C O N T E N T S

OPENING STATEMENTS

	Page
Hon. David Schweikert, Arizona, Chairman	1
Hon. Bill Pascrell, New Jersey, Ranking Member	2
Advisory of October 19, 2023 announcing the hearing	V

WITNESSES

Linda Miller, Founder and CEO, Audient Group	5
Amy Simon, Principal, Simon Advisory	17
Rebecca Shea, Director of Audits, Forensic Audits and Investigative Services, U.S. Government Accountability Office	27
Robert Asaro Angelo, Commissioner, New Jersey Department of Labor and Workforce Development	54

MEMBER QUESTIONS FOR THE RECORD

Member Questions for the Record to and Responses from Linda Miller, Founder and CEO, Audient Group	83
Member Questions for the Record to and Responses from Rebecca Shea, Director of Audits, Forensic Audits and Investigative Services, U.S. Government Accountability Office	88

PUBLIC SUBMISSIONS FOR THE RECORD

Public Submissions	114

Updated Timing

United States House Committee on
Ways & Means
CHAIRMAN JASON SMITH

FOR IMMEDIATE RELEASE
October 12, 2023
No. OS-03

CONTACT: 202-225-3625

Chairman Smith and Oversight Subcommittee Chairman Schweikert Announce Subcommittee Hearing on Investigating Pandemic Fraud: Preventing History from Repeating Itself

House Committee on Ways and Means Chairman Jason Smith (MO-08) and Oversight Subcommittee Chairman David Schweikert (AZ-01) announced today that the Subcommittee on Oversight will hold a hearing on the historic levels of pandemic fraud and how to prevent such unlawful activities in the future. The hearing will take place on **Thursday, October 19, 2023, at 10:00 AM in 1100 Longworth House Office Building.**

Members of the public may view the hearing via live webcast available at https://waysandmeans.house.gov. The webcast will not be available until the hearing starts.

In view of the limited time available to hear the witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit written comments for the hearing record can do so here: WMSubmission@mail.house.gov.

Please ATTACH your submission as a Microsoft Word document in compliance with the formatting requirements listed below, **by the close of business on Thursday, November 2, 2023**. For questions, or if you encounter technical problems, please call (202) 225-3625.

Updated Timing

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission but reserves the right to format it according to guidelines. Any submission provided to the Committee by a witness, any materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission not in compliance with these guidelines will not be printed but will be maintained in the Committee files for review and use by the Committee.

All submissions and supplementary materials must be submitted in a single document via email, provided in Word format and must not exceed a total of 10 pages. Please indicate the title of the hearing as the subject line in your submission. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record. All submissions must include a list of all clients, persons and/or organizations on whose behalf the witness appears. The name, company, address, telephone, and fax numbers of each witness must be included in the body of the email. Please exclude any personal identifiable information in the attached submission.

Failure to follow the formatting requirements may result in the exclusion of a submission. All submissions for the record are final.

ACCOMMODATIONS:

The Committee seeks to make its facilities accessible to persons with disabilities. If you require accommodations, please call 202-225-3625 or request via email to WMSubmission@mail.house.gov in advance of the event (four business days' notice is requested). Questions regarding accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Note: All Committee advisories and news releases are available on the Committee website at http://www.waysandmeans.house.gov/.

###

INVESTIGATING PANDEMIC FRAUD: PREVENTING HISTORY FROM REPEATING ITSELF

THURSDAY, OCTOBER 19, 2023

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT,
COMMITTEE ON WAYS AND MEANS,
Washington, DC.

The subcommittee met, pursuant to call, at 10:03 a.m., in Room 1100, Longworth House Office Building, Hon. David Schweikert [Chairwoman of the Subcommittee] presiding.

Chairman SCHWEIKERT. Good morning, and welcome to today's oversight hearing on the investigating pandemic fraud and preventing history from ever repeating itself again.

We have all seen the headlines: biggest fraud in a generation. Easy money. The great grift. These terms were used to describe the historic amount of fraud that has plagued the government assistance program during the COVID–19 pandemic. It is my hope today that we will deliver deep—that we will dive deeper into how. And this is the key point. Walk us through not only your fixes, particularly the technology discussion some of you have, but how was it done?

I think, for many of us, the visualization in our heads of how do you move billions of dollars, how—in some of the details we are going to hear, how so much of it ended offshore. In many ways, this is not partisan; we are actually trying to understand how American people that needed the help and governments who are struggling to finance it, where did the money go and how was it stolen?

The goal of the hearing is to—is not to cast blame on one side of the aisle or the other. Rather, my hope is in this hearing we will help identify and—identify corrective action needed to prevent massive fraud from happening when resources are pushed out in the future.

There was a great sense of urgency to get a massive amount of resources out the door into the pockets of Americans who were in need. For example, in the first 14 days of the Paycheck Protection Program, the Small Business Administration distributed over $300 billion of loans. The unprecedented amount of spending naturally made benefit programs more susceptible to bad actors. We know the unemployment insurance fraud totaled at least—and we are having a running dispute, and all of you, I will ask to speak to this if you think you have a more accurate number—100 to $135 billion,

and the IRS now has issued a moratorium on the Employer Retention Tax Credit due to its fears of significant fraud.

There are too many stories of pandemic fraud in today's media. Can I give you one example? For one instance—and you will love this one—the FBI discovered a Nigerian state government official who was in possession of stolen bank credit card and tax information of numerous Americans and used these identities to obtain $350,000 worth of unemployment benefits from several states. But he is just one example of scores of foreign fraudsters that use stolen identification to loot the aid intended to help Americans.

In other cases, a man from Michigan who was on parole when he filed dozens of fraudulent unemployment claims using the identity of federal and state inmates who were not eligible to receive the benefits,—he obtained their personal information using the website off the dark web by falsely claiming he could help improve their credit ratings. This man has since pled guilty to wire fraud and aggravated identity theft.

And those examples only start to scratch the surface. We must understand how the fraud was committed so we can stay ahead of the criminals and use whatever—the most advanced technology available to stop this in the future.

I will encourage that the Pandemic Response Accountability Committee formed by an—the committee formed an initiative by data scientists using artificial intelligence and a risk model to analyze pandemic spending and identify abnormalities. This type of data sharing can help law enforcement agencies pursue fraud investigations. It is my hope that using tools like this will not only help hold criminals accountable for their actions in the past but will also guide the future efforts of Congress.

We recognize three things. There is a dispute over the dollar amounts. We have already spent some time trying to blame each other, whether it be on the partisan facts—that is not the goal of this committee. But the third thing, it is the single thing I think is most important to Mr. Pascrell and myself: how did they do it; what do we implement so it never happens again?

Chairman SCHWEIKERT. And with that I yield to the ranking member, Mr. Pascrell.

Mr. PASCRELL. Thank you, David. Good morning, everybody. It is good when you see bipartisanship. It happens so infrequently up here. And David, thank you for your selection of the witnesses today.

I want to welcome our witness, Rob Asaro-Angelo, New Jersey's labor commissioner. He is a very good friend, hard worker, relentless, and he has done a great job, even under your estimates——

Chairman SCHWEIKERT. Do you know everyone in New Jersey? [Laughter.]

Mr. PASCRELL [continuing]. In administering and modernizing our state's unemployment insurance program during the worst employment crisis in generations.

So, Congress acted decisively in the face of historic adversity to keep Americans safe. And I think you heard the chairman reiterate that. Our unemployment aid kept families together, and it saved lives. More than 1.5 million Garden Staters received unemployment from March the 20th to September 2021. It stopped mortgage

defaults, kept the electricity on, put food on tables and in children's stomachs.

Then, in March of 2021, we passed the American Rescue Plan because the crisis was not over. It included unemployment aid, strong enforcement protections—we thought—to fight fraud and recover taxpayer dollars. President Biden used those protections to prosecute frauds. States have recovered nearly $1.2 billion so far, so enforcement is working.

As Rob will testify, New Jersey put these dollars to excellent use, bringing our system into the 21st century with a focus on accessibility and security. In the Federal Government, we have not even done that. I don't care whether there is a Democratic president or is a Republican president, we have failed the Nation by not keeping up to the times.

The majority claims to care about misuse. I believe they are—in their souls. But the other side sought to rescind unspent American Rescue Plan money funding allocated to crack down on fraud, to recover overpayments, and improve unemployment insurance security.

Our pandemic measures exceeded expectations. We emerged stronger than any other country in the world. Every job lost during the pandemic was recovered. All our economic output loss is regained. Job growth is at a 40-year high. Unemployment is at a 54-year low. I think the economy is booming, and I think there is a long way to go. And they are not contradictory.

I am happy to work together with our chairman to ensure Federal dollars are well spent. Fraudsters must be held accountable, period. Our witness from New Jersey deeply understands this, Mr. Chairman, the unemployment insurance fraud, has ideas on how we could prevent this in the future.

It is imperative that, when seeking solutions, we refrain from shaming our workers and lying about our strong economy. And what is, is. The truth is our actions during the pandemic saved lives and saved the American economy.

Mr. PASCRELL. Mr. Chairman, thank you for putting us together this morning, and I look forward to the—hearing from the witnesses.

Chairman SCHWEIKERT. Thank you, Mr. Pascrell.

Would you like a vanilla cappuccino? [Laughter.]

Mr. PASCRELL. Thank you very much, Mr. Chairman.

Chairman SCHWEIKERT. And now to the big chairman, Chairman Smith.

Mr. PASCRELL. Do you have a nomination? [Laughter.]

Chairman SMITH. "The big chairman" just kind of makes me nervous. But I would like a cappuccino, if I could have one. I am just kidding. More like a monster drink. [Laughter.]

Chairman SMITH. But thank you, Chairman Schweikert, Ranking Member Pascrell. It is always a pleasure to be with you all.

Part of our oversight responsibilities here in Congress is to assess when the fraudulent use of tax dollars occurs, and account for what has been lost. But the American taxpayer also expects us to put an end to as much of that fraud as—that we can to hold the fraudsters accountable and, better yet, stop the illegal activity before it happens. That is why I appreciate that today's hearing is

forward looking. We are focusing on not just the when and where, but on the how and why fraud occurs, because that is how we get to the solutions that will protect the taxpayer and the rightful beneficiaries of these programs.

The numbers are staggering. A recently-released Government Accountability Office report pegs the cost of fraud in the pandemic-era unemployment insurance program at 100 billion to 135 billion, doubling GAO's previous estimate that the Comptroller General shared with this committee in February. Some outside experts put the level of improper payments as high as 400 billion. And that is just in the UI programs. As I noted in our hearing on this issue back in February of this year, this is the greatest theft of taxpayer dollars in American history.

We also know the Employee Retention Tax Credit program has been an easy and convenient target for criminals seeking to defraud the government as well as small businesses to such an extent that, as we discussed at our oversight hearing in July, the ERTC program is on the IRS's Dirty Dozen list of worst scams in the country. In fact, as of the end of July the IRS has initiated 252—252—investigations covering over 2.8 billion of potentially fraudulent ERTC claims from 2020 to 2022.

To be clear, the type of criminals we are talking about are not just homegrown fraudsters or lone wolves looking to prey on unsuspecting beneficiaries. We are talking about transnational organized criminal enterprises. Moreover, we have found that, in cities that were able to crack down on the UI fraud they saw occurring, violent crime in those same localities went down, meaning these were more violent criminals committing this fraud. In Baltimore, they found that 60 percent of violent criminals were also committing some type of COVID–19 fraud. When they started prosecuting COVID–19 fraud cases, they saw a 20 percent reduction in homicides—20 percent reduction in homicides.

I appreciate the fact that we have witnesses today from both within government and outside of government. With an estimated $280 billion in stolen COVID–19 relief funds, we need to be seeking input from as many experts as we can to bring as many perspectives as we can to build a more robust defense against fraud. I look forward to the solutions that will come from today's discussions.

Chairman SMITH. And I yield back to you, Mr. Chairman.

Chairman SCHWEIKERT. Thank you, Chairman Smith. One last bit of business to do. I have two vanilla cappuccinos left. Raise your hand if you want one of them. I got one sold and—no one else? They are really good. Okay, I got the two sold.

All right. Linda Miller is the founder and CEO of Audient Group. Did I say that right?

Ms. MILLER. Audient Group.

Chairman SCHWEIKERT. Audient Group, okay. Well, it is a weird spelling.

She also serves as the executive director of the Pandemic Response Accountability Committee and spent 10 years working for the Government Accountability Office.

Amy Simon is a principal for Simon Advisors. She is—previously served as the acting deputy secretary for employment and training administration at the U.S. Department of Labor.

Rebecca Shea, which is a famous name in the Scottsdale Phoenix area, so she says, not related to the name, is the director of audits and forensic audits and investigative services at the U.S. Government Accountability Office.

And Robert Angelo is the commissioner of the New Jersey Department of Labor and Workforce Development.

Thank you for joining us today. You each have five minutes.

Also, to—last thing, I want to echo Mr. Pascrell's—you are a terrific panel. We are here to do something a little different than we often do; we are here to listen.

Ms. Miller, start to educate us.

STATEMENT OF LINDA MILLER, FOUNDER AND CEO, AUDIENT GROUP

Ms. MILLER. Thank you so much. It is a real pleasure to be here today in this forward-looking hearing with this committee. I am really excited.

My name is Linda Miller, and I have, as Chairman Schweikert mentioned, started my own consultancy working on fraud risk management. But I have spent my entire career in the government fraud space, including serving as deputy executive director of the Pandemic Response Accountability Committee.

In talking about what happened during the pandemic when it comes to fraud, there was a combination of inadequate oversight and internal controls, large-scale organized fraud rings, and antiquated data and information systems that contributed to the widespread and massive fraud that we saw during the pandemic. Going forward, two significant problems must be solved.

One, fraud prevention is simply not a priority for Federal and state agencies. The pandemic highlighted this critical gap.

And two, the use of data in government is broken. Data is an essential tool, and the fight against fraud and sharing data and using it to prevent fraud is simply not working.

My written statement today outlines five key actions Congress can take to help ensure history doesn't repeat itself. Today, I am going to highlight a couple of those.

First, a dedicated anti-fraud office with senior-level authority should be created. Agencies struggle with competency and fraud and data analytics. They struggle with data sharing, and they struggle with a lack of incentives to allocate resources to these activities. An all-of-government strategy should be established and implemented by a well-funded, centralized entity with the authority to effect real change. Such an office would have the necessary skills and resources to work solely on addressing the data, accountability, and technology challenges agencies face at every level of government.

As part of this office Congress should direct the creation of a fraud analytic center of excellence modeled on the PRAC's Pandemic Analytic Center of Excellence. A centralized analytics hub in the management side of government would create an economy of scale, and would place a data-driven emphasis on fraud prevention, where it can be the most effective.

Second, we must adopt approaches that are used in the private sector. Conventional wisdom today holds that you can promote cit-

izen access to government services or you can prevent fraud, but you cannot do both. This trade-off doesn't exist in the private sector, and it shouldn't in government. Banks effectively balance the competing business imperatives of attracting and retaining customers and preventing fraud every day. Both are vitally important to their bottom line.

Part of the challenge lies in outdated laws, and—that limit agencies' ability to use data and prevent fraud, especially given the rise of data breaches and the epidemic of identity theft that we are seeing today.

Developing innovative projects in partnership with the private sector can help mature the government's capacity to prevent fraud. For example, the Senate Appropriations Committee's fiscal year 2024 financial services bill contains language directing Treasury to lead a public-private partnership to counter the increasing threats of financial fraud, which will facilitate information sharing between government and private sector, develop best practices, and encourage innovations in fraud prevention.

Another approach Congress should consider is the creation of a regulatory sandbox that would allow the private sector to work with agencies on data-driven fraud prevention approaches with a degree of assurance that those won't run afoul of statutory and regulatory requirements such as privacy laws that limit the use of data for fraud prevention.

Third, agency leaders need incentives to prevent fraud. Company CEOs respond to the demands of their customers and their shareholders. As citizens, we are government's customers and its shareholders, and we do not demand fraud prevention, we demand timely access to services. Agency leaders need incentives to prevent fraud. Congress can incentivize agency leaders by holding regular hearings to discuss actions to prevent fraud, building fraud prevention into the performance metrics of those leaders, and measuring their activities against an established benchmark.

A word of caution, though, on incentives. The hidden nature of fraud makes it easy to ignore. If agencies are only measured on the amount of fraud they have, they will establish meaningless fraud indicators and then give the false impression that fraud is controlled. Incentives in fraud prevention should be focused on the actions that agencies are taking and the rigor with which they are measuring the effectiveness of those actions.

And finally, we need dedicated funding set aside for fraud prevention and large spending bills. The Bipartisan Infrastructure Law and the Inflation Reduction Act both contained enormous grant and loan programs but provided no funding or requirements for safeguarding the integrity of those funds. Fraud actors will target those programs with the coordinated fraud schemes that they did during the pandemic.

Data and analytics can be a game changer. Massive amounts of third-party data can be mined and leveraged to identify suspicious indicators. Establishing dedicated funding for fraud prevention in these spending bills will provide the focus and resources needed.

When it comes to fighting fraud, an ounce of prevention really is worth a pound of cure. We must put fraud prevention tools in the

hands of government leaders and hold them accountable to prevent history from repeating itself. Thank you.

[The statement of Ms. Miller follows:]

Subcommittee on Oversight of
the House of Representatives Committee on Ways and Means

Hearing: Investigating Pandemic Fraud – Preventing History from Repeating Itself

Testimony of Linda Miller

October 19, 2023

Subcommittee Chairman Schweikert, Ranking Member Pascrell, and esteemed members of the Subcommittee, I am pleased to be here today to share my perspectives on enhancing the government's efforts to prevent, detect, and respond to fraud. I am the Founder and CEO of a boutique consultancy specializing in fraud risk management. I also bring to bear my former experience both as the Deputy Executive Director of the Pandemic Response Accountability Committee, or PRAC, and as an Assistant Director in the Forensic Audits and Investigative Service group at the Government Accountability Office (GAO).

The nearly $5 trillion in government relief spending during the COVID-19 pandemic — much of which was disbursed as direct payments to citizens — created the perfect storm for fraud. A combination of inadequate oversight and internal controls, large-scale organized fraud rings, and antiquated data and information systems contributed to the massive, widespread fraud we saw during the pandemic. Agencies were unprepared for the fraud they encountered largely due to a lack of attention on fraud risks. GAO issued its Framework for Managing Fraud Risks in Federal Programs in 2015, but regrettably little attention was paid to establishing the preventative controls GAO called for to manage fraud risks.

Today, fraud actors have at their disposal massive amounts of personal information on nearly every American. Coupled with sophisticated technological tools, this makes committing fraud far easier than it's ever been. Congress has the opportunity

to demonstrate a commitment to preventing fraud in the future, following the devastating fraud losses experienced during the pandemic.

My testimony today focuses on five key actions Congress can take to help ensure history doesn't repeat itself: 1) Create a dedicated antifraud office; 2) explore ways to enhance data-driven fraud prevention; 3) revise improper payment laws to focus on high-risk programs; 4) incentivize fraud prevention; and 5) earmark fraud prevention funding in large spending bills.

Create a Dedicated Antifraud Office with Senior Level Authority

Senior levels of government have long neglected the prevention of fraud and improper payments. To change that, focused senior level attention is needed. Agencies struggle with competency in fraud and data analytics, they struggle with data sharing, and they struggle with a lack of incentives to allocate resources to these activities.

An all-of-government strategy should be established and implemented by a well-funded, centralized office with the authority to effect real change. A dedicated antifraud office would have the necessary skills and focus to work solely on addressing the data, accountability, and technology challenges facing agencies at every level of government.

A dedicated federal antifraud office would serve as the focal point for identifying emerging technology, establishing guidance, and providing technical assistance to help agencies adopt new data analytics technology and techniques. The United Kingdom established such an office in 2018 and has seen enhanced focus on program integrity as a result.

As part of this office, Congress should direct the creation of a fraud analytics center of excellence. Modeled on the PRAC's Pandemic Analytics Center of Excellence, which can only be used by oversight entities to address fraud that has already

occurred, a similar analytics center of excellence on the management side of government would allow for a data-driven emphasis on fraud *prevention*, where fraud risk management is most efficient and effective.

Today, agencies spend valuable time and money building redundant analytics systems and buying commercial tools duplicatively, wasting taxpayer dollars. Centralizing this effort would save taxpayer money by creating an economy of scale.

Treasury has made progress enhancing its Do Not Pay system along with its Payment Integrity Center of Excellence. With additional funding and a mandate to create a centralized, data analytics capability, this system could establish an unprecedented government-wide data analytics platform to identify and prevent potential fraud and improper payments across government programs.

Explore Ways to Enhance Data-Driven Fraud Prevention

Conventional wisdom holds that you can promote citizen access to government services or you can prevent fraud, but you can't do both. This tradeoff doesn't exist in the private sector, and it shouldn't in government. Banks effectively balance the competing business imperatives of attracting and retaining customers and preventing fraud every day. Both are vitally important to their bottom line. But in government, we often only focus on attracting and retaining customers, erroneously thinking that if we focus on preventing fraud, we will impede citizen access to needed services.

The government lags the private sector in the use of technology to identify and prevent fraud. During the pandemic, fraud actors saw an enormous opportunity to exploit this weakness. State and federal agencies were and are vulnerable to fraud because they lack the tools necessary to detect fraud patterns. One example: a cyber intelligence research firm identified 259 variations of a single email address used by

a crime ring to create accounts on state and federal websites with the intent to carry out fraud. Government agencies must begin to catch up with the technology used by sophisticated fraud actors.

Part of the challenge lies in outdated laws, including the Fair Credit Reporting Act (FCRA) and the Privacy Act. These laws severely limit agencies' ability to use data to prevent fraud, especially given the rise of data breaches and the epidemic of identity-theft based fraud perpetrated by sophisticated organized criminal groups. Rapid technological developments, digitalization and datafication of society and the economy require innovative regulatory approaches, in addition to traditional laws, regulations and regulatory policies. The tension between privacy protection and fraud prevention creates an untenable paralysis within government that fraudsters happily exploit.

Innovative approaches to assisting agencies use data include:

- **Statutory code of practice for sharing private information.** Data sharing is an enormous challenge in the government, and for many agencies, the perceived risks of getting it wrong— reputational damage or enforcement action by the regulator— outweigh the benefits that can be gained from data sharing, leading to missed opportunities for innovation and improved fraud prevention. A code of practice, like one created in the U.K., can help provide a common understanding of best practice in data sharing.
- **Regulatory sandbox**[1]. A regulatory sandbox would allow the private sector to partner with agencies on data-driven fraud-prevention approaches with a

[1] A regulatory sandbox is a set of rules and appropriate safeguards, usually summarized in writing and published, that allows for live, time-bound testing of innovations under a regulator's oversight. A sandbox creates a conducive and contained space for experimenting with innovations at the edge or even outside of an existing regulatory framework.

degree of assurance that the experimental and testing phases are unlikely to run afoul of statutory or regulatory requirements.

- **Public-private partnership with financial institutions**. Partnering with financial institutions, who have more mature fraud prevention tools, agencies can learn how to balance the need to ensure timely access to government services with effective fraud prevention. The Senate Appropriations Committee's FY24 Financial Services and General Government bill report contains language directing the Treasury Department to lead a multisectoral whole-of-society effort to counter the increasing threats associated with financial fraud. This public-private partnership will encourage information sharing between government and private sector participants, develop best practices for relevant stakeholders, and encourage innovations in counter-fraud technologies, data-analytics, and approaches. I encourage the Subcommittee to engage with its Senate counterparts to help enact this provision.

Piloting the implementation of some of the more innovative data-driven tools in use in the financial sector, within the context of a regulatory sandbox, would yield meaningful progress. Congress can also use the results of these efforts to reform the laws that impede data-driven fraud prevention, proving that you can prevent fraud while protecting privacy and maintaining timely access to government services.

Revise Improper Payment and Fraud Prevention Laws to Focus on High-Risk Programs

The current approach to preventing fraud and improper payments in the federal government is costly, inefficient, and ineffective. As currently written, the Payment Integrity and Information Act (PIIA) creates burdensome compliance requirements on low-risk agencies and programs but does little to reduce improper payments made by larger, higher risk programs.

Government cannot afford to waste limited resources on low-risk activities. The Congressional Research Service analyzed 2017 data and found that 85 to 98 percent of all improper payments were made by 20 programs identified as high priority following Executive Order 13520, which established criteria for such programs.

Yet today, all agencies with programs of at least $10 million are currently required to undertake burdensome compliance activities, which they do with a check-the-box approach, wasting valuable time and resources that could be better spent on data- and outcome-oriented efforts.

Real progress in areas of fraud and improper payments can only be made by transitioning to a risk-based, data- and outcome-focused approach. Those agencies with programs susceptible to fraud and improper payments should be required to implement proactive, intelligence- and analytics-driven initiatives to prevent, detect, and respond to fraud threats and demonstrate meaningful progress in measuring and reducing improper payments.

Amending PIIA to eliminate burdensome requirements on low-risk programs, setting a threshold (e.g., $50 billion or more in outlays) and requiring those programs above that threshold to implement advanced analytics programs for fraud prevention and detection will help focus attention on the areas of highest risk, thereby enhancing both effectiveness and efficiency.

Incentivize Fraud Prevention

Try to imagine a scenario where the CEO of a private sector company could save millions of dollars by obtaining the needed data to verify the accuracy of customer-provided information, but simply does not do so. It's hard to fathom shareholders would accept that. So why is this the case in government?

Because as citizens, we are both the government's customers and its shareholders. And we hold government accountable for little other than quickly providing us the

benefits we are entitled to or eligible for. When citizens complain about wait times or complex application processes, agency leaders listen. In recent years, government agencies have prioritized "customer experience." In fact, an entire industry focused on customer experience (it even has an acronym, CX) is at work across government, making things easier for customers to navigate.

This problem must be addressed at the root—agency leaders need more institutional incentives to manage fraud, waste, and abuse in their programs more systematically. They must be held accountable for using data and tools to prevent fraud, waste, and abuse before it happens.

That accountability should start with benchmarking what proactive fraud prevention programs agencies should have in place. Currently agencies employ a wide range of tools and activities in service to fraud prevention. Some of the larger programs have some of the less-mature fraud risk programs and vice versa. A centralized office could dedicate the time and expertise to establishing benchmarks and providing technical assistance to agencies to put the needed tools in place.

Congress can also incentivize agency leaders by holding regular hearings with agency leaders to discuss their actions to prevent fraud. A word of caution on incentives: The hidden nature of fraud makes it easy to ignore. If agencies are only measured on the "amount of fraud" they have, the unintended outcome will be that agency leaders will simply look the other way, underreporting their fraud by establishing meaningless definitions and giving the false impression that fraud is well controlled. *Incentives in fraud prevention should be focused on the actions agencies are taking and the rigor with which they are measuring the effectiveness of those actions.*

Building fraud prevention into agency leaders' performance metrics and those of their managers, measuring their activities against an established benchmark,

scheduling regular "fraud hearings" and requiring agency leaders to share how they are working to prevent and detect fraud could all help incentivize fraud prevention.

Earmark Fraud Prevention Funds in Large Spending Bills

Preventing fraud and improper payments is a data game. Large spending bills like the Bipartisan Infrastructure Law and the Inflation Reduction Act contained enormous grant and loan programs but provided no funding or requirements for safeguarding the integrity of those funds. Like many pandemic programs, fraud actors will target those programs with coordinated fraud schemes. Data and analytics can be a game changer, for example:

- The acceleration of machine learning and artificial intelligence tools offers government agencies the ability to identify fraud schemes quickly.
- Natural language processing text analytics engines can identify duplicate passages in grant applications in seconds.
- Massive amounts of third-party data can be mined and leveraged to identify past criminal activity and other suspicious indicators related to applicants.
- Third-party data analysis can also identify patterns indicative of stolen or synthetic identities used in grant, loan, and benefit applications.
- Social network analytics can identify the relationships between applicants that could indicate the existence of a fraud ring.
- Device metadata, such as geolocation, can also be mined to identify potential fraud indicators. And all this data analysis can be done in seconds with the tools available today.

To protect taxpayer resources, government agencies must invest in the tools needed to fight fraud. Establishing dedicated funding for fraud prevention to accompany large spending bills and directing agencies to establish metrics for preventing fraud actors from stealing the funds provided in any large new spending bill will provide the needed focus on fraud prevention.

These observations and recommendations are the result of my decades of work supporting fraud risk activities in the federal government. There were simple steps that could have been taken to minimize the extent of fraud we saw in many of the pandemic response programs. Hopefully, we can take the lessons learned from that experience to ensure we don't suffer that extent of fraud in the future.

Chairman SCHWEIKERT. Ms. Miller, that was remarkably helpful.

Ms. Simon.

STATEMENT OF AMY SIMON, PRINCIPAL, SIMON ADVISORY

Ms. SIMON. Chairman Schweikert, Ranking Member Pascrell, thank you for the opportunity and invitation to testify today.

As a former leader in the U.S. Department of Labor's Employment and Training Administration during the pandemic, I was a firsthand witness to both the economic devastation of the pandemic and to the extraordinary legislative policy and operational responses contained in multiple pieces of legislation, starting with the CARES Act. And later, as an unemployment insurance claimant and victim of identity theft, I was a firsthand witness to the system's flaws and operational weaknesses. And so I believe this question of what do we do next and how do we move forward is incredibly timely, and I appreciate the committee's attention.

My prepared remarks highlight the incredible scale of both the pandemic benefits and the scale of fraud. And due to this hearing's focus on fraud, I did not address the many adjacent and substantive policy issues in unemployment insurance. That would certainly need to be part of a more comprehensive conversation. Instead, in my opening statement, I would like to highlight just two themes.

First, I often sense an inherent tension that fraud detection and prevention and benefit accessibility are opposing goals. This is a false dichotomy. It was often eligible claimants who waited for months on end, while fraudsters easily stole millions. It was often eligible claimants who found out that their benefit accounts had been drained when fraudsters socially engineered access. It was often eligible claimants who found out that they couldn't get benefits because a fraudster had already applied in their name. These claimants are the heart of the program's mission to provide temporary partial income replacement for workers out of a job for no fault of their own. If you care about the program, you need to care about fraud. It does not have to be one or the other.

Second, I think that unemployment insurance pandemic fraud lessons are broader than just unemployment insurance. Three quick examples.

Fraud is constantly evolving, targeted, and agile. Unemployment insurance fraudsters repeatedly went to public sources for tutorials and help on how to more effectively accomplish their fraud schemes. Government's response was not evolving, targeted, or necessarily agile, especially at the beginning of the pandemic. Static solutions to dynamic threats are not going to move the needle quickly enough in this environment.

Second, pandemic fraud did not stay in the pandemic. Fraudsters are paying attention, and we do not have the luxury of returning to pre-pandemic norms. Mission success and program performance metrics must reflect the extent to which benefit programs are or are not managing fraud risks effectively.

And third, there are potential national security implications for domestic benefit programs when billions of fraudulent dollars flow through them to unfriendly international or even state-sponsored

cyber crime groups. I believe there are active roles for Congress to play on each of these fronts.

I appreciate the opportunity to testify and look forward to your questions.

[The statement of Ms. Simon follows:]

TESTIMONY OF AMY SIMON

PRINCIPAL, SIMON ADVISORY LLC

BEFORE THE U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON OVERSIGHT

October 19, 2023

I. Introduction

As a member of the United States of Department of Labor (DOL) Employment and Training Administration (ETA) leadership in early 2020, I witnessed the pandemic's economic devastation to American workers and then the legislative, policy, and operational emergency policy unemployment benefit responses. Later, as an unemployment insurance claimant and identity theft victim – like many others – I witnessed the infrastructure and fraud prevention gaps in the system's operational realities. Now, working in unemployment insurance policy and technology, I hope that the lessons of this experience, particularly around fraud, can be the catalyst for significant policy and operational change in the program.

Much of this content is drawn directly from a forthcoming paper, with co-author Matthew Weidinger, on the unemployment insurance pandemic fraud experience and from previously published work.[1]

II. Unemployment Insurance Pandemic Fraud Retrospective: What and Why

The coronavirus pandemic tested the nation's unemployment benefits system more than any prior recession. Not only did far more individuals file claims for weekly benefits than ever before, but lockdowns and mass layoffs concentrated those record claims starting in March 2020, creating an unprecedented surge in demand for benefits that quickly rose to an apparent 33 million claims by June 2020.[2] That soaring demand for assistance, accompanied by unprecedented federal benefit expansions, also created unprecedented opportunities for everyone from small-time crooks to international criminal organizations to defraud the nation's unemployment benefits system.[3]

---

[1] Amy Simon. American Enterprise Institute, "Unemployment Insurance at a Crossroads: Tracing Program Design During and Beyond COVID-19." October 20, 2021, https://www.aei.org/research-products/report/unemployment-insurance-at-a-crossroads-tracing-program-design-during-and-beyond-covid-19/

[2] Department of Labor, "Unemployment Insurance Weekly Claims," July 9, 2020, https://oui.doleta.gov/press/2020/070920.pdf

[3] For a discussion of the involvement of organized criminal groups, see: Inskit Group, "Termination of Federal Unemployment Programs Represents Turning Point for Fraudsters," *Recorded Future*, October 28, 2021, https://www.recordedfuture.com/termination-federal-unemployment-programs-turning-point-fraudsters. Cezary Podkul, "How Unemployment Insurance Fraud Exploded During the Pandemic", ProPublica, July 26, 2021, https://www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic. Matt Weidinger, "Did Russian Gangs Steal More from US Taxpayers Than We Gave Ukrainians to Defend Themselves?" *Washington Examiner*, November 18, 2022, https://www.aei.org/op-eds/did-russian-gangs-steal-more-from-us-taxpayers-than-we-gav-ukrainians-to-defend-themselves

The scale of improper spending and outright fraud is only now coming into clearer focus. Official federal estimates, while still preliminary, are astonishing. Based on an assumed improper payment rate of more than 21 percent, government officials have conservatively estimated at least $191 billion in improper payments during the pandemic. However, that figure is expected to rise, likely to $240 billion or more, following a recent Government Accountability Office (GAO) report that found that the Pandemic Unemployment Assistance (PUA) program had an even higher improper payment rate of almost 36 percent.[4] GAO separately estimates between $100 billion and $135 billion in unemployment benefits were lost to fraud during the pandemic, or approximately one in every seven dollars in benefits paid.[5]

Problems with state technology systems, now well-known, spiked alongside rapidly ascending claims in mid-2020.[6] Soaring claims—including by individuals and groups bent on defrauding the system—compounded underlying administrative issues and novel factors related to the pandemic that resulted in enormous stress on the system and long waits for rightful claimants. During the 18 months between when the pandemic struck and temporary federal programs expired in early September 2021, nearly 1.6 billion weekly state and federal unemployment benefit checks were paid.[7] The cost of these benefits was equally unprecedented: approximately $900 billion in total unemployment benefits was distributed between March 2020 and September 2021, including $700 billion in federal benefits.[8]

The DOL IG, in testimony to Congress in February 2023, provides the most recent government estimate of how much of that spending resulted from improper payments. Applying DOL's December 2022 estimate of a 21.52 percent improper payment rate for the state UI program and selected federal programs, the IG suggested the "low end" for improper payments was $191 billion.[9] However, that estimate didn't include the subsequent and even higher 35.9 percent PUA improper payment rate that DOL reported in August 2023.[10] When that higher PUA improper payment rate is factored in, overall improper payments could easily rise to $240 billion or more.[11]

---

[4] Department of Labor, "PUA Improper Payment Rate Report," https://oui.doleta.gov/unemploy/pdf/Pandemic_Unemployment_Assistance_Improper_Payment_Rate_Report.pdf

[5] Government Accountability Office, "Unemployment Insurance: Estimated Amount of Fraud During Pandemic Likely Between $100 Billion and $135 Billion," September 12, 2023, https://www.gao.gov/products/gao-23-106696

[6] For example, see Minyvonne Burke, "Coronavirus: State unemployment websites crash as applications surge," NBC News, March, 18, 2020, https://www.nbcnews.com/news/us-news/coronavirus-state-unemployment-websites-crash-applications-surge-n1162731

[7] Department of Labor, "Weeks Claimed in All Programs (Expanded)," https://oui.doleta.gov/unemploy/docs/allprograms.xlsx

[8] Government Accountability Office, "Pandemic Programs Posed Challenges, and DOL Could Better Address Customer Service and Emergency Planning," https://www.gao.gov/assets/gao-22-104251.pdf

[9] US Department of Labor Inspector General, Testimony before the US House Committee on Ways and Means, February 8, 2023, https://www.oig.dol.gov/public/testimony/02082023.pdf

[10] US Department of Labor, "PUA Improper Rate Report," August 21, 2023, https://oui.doleta.gov/unemploy/pdf/Pandemic_Unemployment_Assistance_Improper_Payment_Rate_Report.pdf

[11] For a review, see Matt Weidinger, , "Up to $135 Billion in Pandemic Unemployment Fraud – and Still Counting," Real Clear Policy, September 29, 2023, https://www.realclearpolicy.com/articles/2023/09/29/up_to_135_billion_in_pandemic_unemployment_fraud__and_still_counting_982978.html

Recovery of misspent funds to date has been minimal. According to the September 2023 GAO report, as of May 1, 2023, states had recovered $1.2 billion in fraudulent overpayments and $5.6 billion in nonfraudulent overpayments.[12] While recoveries should continue growing, the nonpartisan Congressional Budget Office (CBO) expects that recoveries of currently-identified fraudulent payments "are likely to be a small percentage of total suspected fraud."[13] The CBO review suggests that at most eight percent of identified losses to pandemic fraud may be recovered. Based on this and the GAO's fraud loss estimate, American taxpayers have likely lost over $100 billion in unrecoverable unemployment insurance fraud.

III. Thematic Elements of Unemployment Insurance Pandemic Fraud Mechanics

Fraudsters used various attacks on state workforce agency websites and systems; these attacks differed markedly from pre-pandemic attempts to defraud the UI system. The following is a non-exhaustive, non-technical overview of the most commonly used attacks.

- *Identity theft*: This was the most common type of fraud, especially in the vulnerable PUA program. After purchasing the relevant information on dark web marketplaces, a fraudster would apply with another identity on the state workforce agency site and direct benefits to a physical address or bank account that they controlled.[14] Resulting benefits would be quickly moved out of the original account to elude any later recovery efforts.[15] This fraud was particularly easy to commit given the massive volumes of available PII from unrelated data breaches. In general, identity theft fraud includes most of the incarcerated claimant schemes, the deceased person schemes, and multi-state application schemes. It also created thousands of victims who learned their identity had been stolen only when they were unable to apply for benefits or when they received an unexpected 1099-G form from the Internal Revenue Service indicating they owed income taxes on unemployment benefits they never applied for or received.[16]

- *Synthetic identity:* Fraudsters could create a false identity from a mosaic of individual data elements assembled to create a non-existent claimant. Crosschecking any individual data element of the application might not reveal discrepancies with existing data, but if a combination of elements were checked, it likely would have revealed serious issues. This includes all schemes in which an individual data element or elements were used and

[12] Government Accountability Office, "Unemployment Insurance: Estimated Amount of Fraud during Pandemic Likely Between $100 Billion and $135 Billion," September 23, 2023, https://www.gao.gov/assets/gao-23-106696.pdf

[13] Congressional Budget Office, "At a Glance: H.R. 1163, Protecting Taxpayers and Victims of Unemployment Fraud Act," March 21, 2023, https://www.cbo.gov/system/files/2023-03/hr1163.pdf

[14] Cezary Podkul, "How Unemployment Insurance Fraud Exploded During the Pandemic", *ProPublica*, July 26, 2021, https://www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic Cezary Podkul, "Congressional Chair Asks Google and Apple to Help Stop Fraud Against U.S. Taxpayers on Telegram," *ProPublica*, March 28, 2022, https://www.propublica.org/article/congressional-chair-asks-google-and-apple-to-help-stop-fraud-against-u-s-taxpayers-on-telegram

[15] Cezary Podkul, "How Unemployment Insurance Fraud Exploded During the Pandemic", *ProPublica*, July 26, 2021, https://www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic.

[16] Greg Iacurci, "Is a scammer getting unemployment benefits in your name? Victims will find out this tax season," *CNBC.com*, February 2, 2022, https://www.cnbc.com/2022/02/02/victims-of-unemployment-fraud-may-find-out-this-tax-season.html

reused many times across claimants or applications.

- *Account Takeover:* Using easily obtained pieces of PII, fraudsters often socially engineered access to an eligible claimant's existing account and changed the bank account information to drain or redirect benefit balances.[17]

- *Phishing Schemes:* Fraudsters would disguise themselves as representatives of state workforce agencies or the US Department of Labor, reaching out to existing claimants via phone, email, or text, and requesting verification codes or missing pieces of PII. Sometimes fraudsters would tell claimants to call a hotline or visit a webpage, either of which would be disguised to appear as the legitimate state workforce agency. Similar groups on social media would impersonate the state agency's visual brand to convince claimants to enter relevant information into a fake site. Any of these methods would generally allow fraudsters to complete an account takeover directly.[18]

- *Benefit Card Skimming:* When states provided benefits on affiliated bank-managed temporary debit cards, they often did not have the additional layers of security necessary to prevent easy theft of the card's access information. Fraudsters could steal the information, create a replica card, and drain the accounts quickly without the claimant's knowledge. In one scheme, card skimming technology installed at an ATM allowed a fraudster to steal and repurpose benefit card balances into hundreds of fake gift cards.[19]

- *Bribery schemes:* Some state staff or contractors accepted payments from third parties to have their fraudulent claims reviewed and approved. State agency workers would solicit or advertise this service, sometimes in coordination with a ring of known co-conspirators. This type of fraud was likely more widespread than is understood as many state agencies do not appear to have deeply investigated their own administrative records for evidence of insider threat.[20]

---

[17] https://www.dol.gov/agencies/eta/UIIDtheft; https://www.finra.org/rules-guidance/notices/22-21#:~:text=In%20connection%20with%20the%20COVID,new%20accounts%20at%20member%20firms; https://abc7news.com/edd-money-stolen-account-hacked-unemployment-benefits-transferring-payments-to-bank/13186896/;

[18] Federal Trade Commission Consumer Alert, "Phishing Scheme targets unemployment insurance benefits and PII", https://consumer.ftc.gov/consumer-alerts/2021/08/phishing-scheme-targets-unemployment-insurance-benefits-and-pii

[19] Ritika Shah, Stephen Council, Angelica Serrano-Roman, Leslie Picker, Jennifer Schlesinger, "How criminals siphoned off unemployment payments directly from recipients' accounts", *CNBC*, July 16, 2021, https://www.cnbc.com/2021/07/16/unemployment-how-fraudsters-stole-benefits-from-recipients-accounts.html; KSNV, "Romanian national gets prison time for skimming hundreds of Nevada DETR debit cards", https://news3lv.com/news/local/romanian-national-gets-prison-time-for-skimming-hundreds-of-nevada-detr-debit-cards

[20] Ryan Jeltema, "2 accused of elaborate insider fraud scheme at Michigan Unemployment Insurance Agency", *ABC12 News*, May 19, 2022 https://www.abc12.com/news/crime/2-accused-of-elaborate-insider-fraud-scheme-at-michigan-unemployment-insurance-agency/article_c30290a8-c638-11ec-907e-cf6acc6ea25e.html; United States Attorney's Office Eastern District of Virginia, "Former Federal Employee Pleads Guilty to $2M Unemployment Benefits Fraud Scheme", https://www.justice.gov/usao-edva/pr/former-federal-employee-pleads-guilty-2m-unemployment-benefits-fraud-scheme; Office of the Inspector General, "OIG Publishes Open Letter Regarding UI Fraud in State Government", https://oig.georgia.gov/press-releases/2023-01-04/oig-publishes-open-letter-regarding-ui-fraud-state-government; United States Attorney's Office Central District Office, "One-Time EDD Employee

- *Self-dealing:* State staff or contractors sometimes applied for and received benefits in their own or others' names while employed. Staff could also run identity theft rings independently and without external parties.[21]

Separate from the attacks themselves, many fraudsters have access to supportive services to enable attacks:

- *Document fraud:* Many types of identity schemes are enabled by the quick production of good-enough documents with necessary data elements. This is no longer limited to image manipulation as the wide availability of 3D printers makes fake document production economical and quick. This also highlights the difficulty of relying on identity documents or liveness checks as the primary keystone for verification.[22]

- *Bot Attacks:* To most efficiently identify both the states likely to pay on fraudulent applications and to rapidly monetize stolen PII, fraudsters did not painstakingly apply for benefits one at a time, but instead engaged in widespread bot attacks seeking vulnerabilities in state systems.[23]

Most of these schemes are not particularly sophisticated nor do they usually require advanced cybersecurity knowledge. Dark web monitoring revealed functional and responsive markets for the intelligence necessary to target attacks and the identity information necessary to monetize the attacks. The full criminal impact of the billions lost to unemployment insurance fraud will likely never be exactly quantified and certainly never fully recovered.[24] Although many of these methods were most effective between March 2020 and early 2021, the attacks on unemployment insurance systems have not necessarily ended when the temporary programs ended. For example, fraudsters have recently and aggressively attacked the Hawaii Disaster Unemployment

---

Sentenced to More Than 5 Years in Prison for Fraudulently Obtaining Nearly $4.3 Million in COVID Relief Funds", https://www.justice.gov/usao-edca/pr/one-time-edd-employee-sentenced-more-5-years-prison-fraudulently-obtaining-nearly-43

[21] Beth LeBlanc, "Unemployment Agency Failed to Limit Access to Sensitive Information, audit says", *The Detroit News*, May 17, 2022, https://www.detroitnews.com/story/news/local/michigan/2022/05/17/michigan-unemployment-agency-failed-properly-limit-access-sensitive-data-information-audit-says/9804085002/; https://audgen.michigan.gov/wp-content/uploads/2022/05/r186059321-8235.pdf; https://audgen.michigan.gov/wp-content/uploads/2022/03/r186031021-7565.pdf

[22] Caresse Jackman, "Fraud Files: Billions in federal funds meant to help unemployed stolen by scammers", *KWOC*, January 2, 2023, https://www.kwqc.com/2023/01/02/fraud-files-billions-federal-funds-meant-help-unemployed-stolen-by-scammers/

[23] Tim Carpenter, "Unemployment insurance fraudsters circling back to Kansas in renewed quest for quick cash", *Kansas Reflector* January 27, 2020, https://kansasreflector.com/2022/01/27/unemployment-insurance-fraudsters-circling-back-to-kansas-in-renewed-quest-for-quick-cash/; "Erin Tiernan, "Charlie Baker blasts 'bot-based fraud' straining Massachusetts unemployment system, thousands to lose coverage next month", *Boston Herald,* November 23, 2020, https://www.bostonherald.com/2020/11/23/charlie-baker-blasts-bot-based-fraud-straining-massachusetts-unemployment-system-thousands-to-lose-coverage-next-month/

[24] Spencer Kimball, "Covid fraud: Street gang in Milwaukee allegedly stole millions to pay for murder, guns and drugs," *CNBC,* August 29, 2023, https://www.cnbc.com/2023/08/29/covid-fraud-gang-allegedly-stole-millions-to-pay-for-murder-guns-drugs.html. Inskit Group, Unemployment Fraud in the Criminal Underground [Report], *Recorded Future,* January 14, 2021, https://www.recordedfuture.com/unemployment-fraud-in-criminal-underground.

Assistance (DUA) program.[25]

IV. Lessons Learned

- *Eligibility self-attestation without an identity verification requirement does not work.*

Self-certification as the statutory eligibility benefits standard was so easily abused that it was demonstrably equivalent to having almost no standard. The PUA program allowed claimants to self-certify their eligibility for benefits while also failing to require proof of prior work or adequate identity verification. As the Department of Labor's Inspector General summarized, PUA's "reliance solely on claimant self-certifications without evidence of eligibility and wages during the program's first 9 months rendered the PUA program extremely susceptible to improper payments and fraud."[26]

- *Require baseline identity verification prior to paying benefits, and tailor identity verification process based on risk.*

Addressing and prioritizing identity verification is a critical step for both the unemployment insurance system and for many public safety net programs beyond unemployment insurance. Lawmakers should consider requiring states to verify all claimants' identities before benefits are paid and requiring that high-risk identities complete additional verification steps. These identity verification requirements can and should be implemented so as not to violate claimants' rights to due process.

- *Require data matching to prevent flagrant abuse.*

Multiple administrations have proposed data-matching mandates, but such requirements have not been made permanent.[27] The OIG listed the lack, or temporary pausing, of such data matching as a key fraud driver during the pandemic. States understandably opted to skip additional data matching when under incredible pressure to dispense benefits. Even apart from statutory changes, the Department should use this moment to identify and rectify deficiencies in the current shared data matching sources, publicize which states are not using the available data sources, and push states on voluntary adoption.

- *Technology gaps often limit policy choices.*

It is difficult to quantitatively define the influence of the flat supplemental FPUC payments ($600 and later $300) on fraud incentives, but it was certainly one of the key drivers. Flat supplemental payments especially when combined with many weeks of retroactive benefits, created an enormous incentive for criminals. This poorly targeted approach resulted from two

---

[25] Daryl Huff, "Hawaii grapples with 'rampant' unemployment fraud, delaying aid to wildfire survivors," *Hawaii News Now*, October 11, 2023, https://www.hawaiinewsnow.com/2023/10/12/hawaiis-unemployment-system-rampant-with-fraud-it-scrambles-help-wildfire-survivors/.

[26] https://www.oig.dol.gov/doloiguioversightwork.htm

[27] There is active legislation that would require states to use key data matches to ensure only intended recipients are able to collect benefits. HR 1163, the *Protecting Taxpayers and Victims of Unemployment Fraud Act*, was approved by the House of Representatives in May 2023.

policy factors — the desire to "make whole" individuals laid off as a result of the pandemic and often government-mandated business shutdowns, and the UI system's inability to provide benefit increases specifically linked to each individual's prior earnings. As many state systems were unable to program an alternative to a flat rate supplement, it appeared the only option. Lawmakers recognized flaws with this approach even before the CARES Act was enacted but proceeded with them anyway.[28] It should be a goal of program reforms to ensure that lawmakers do not have to adopt such similarly blunt policy options; doing so requires attention to streamlining policy, and incentivizing flexible and responsive technology solutions.

- *Improve and simplify the user experience for all stakeholders.*

The incredibly painful user experience during the pandemic highlights the need for simpler, clearer, functional UI technology. The program's very technical policy nuances and historical technology underinvestment made user experience a lower-tier priority. The emphasis of much user experience improvement has been public, claimant-facing plain language efforts. Although important, other unemployment insurance stakeholders' user experience needs should also be considered.

- *Give the Inspector General permanent statutory access to all state UI records for investigations.*

Another important reform is to provide the DOL Inspector General permanent access to all state unemployment benefit records (that is, including on state UI, and when payable, federal unemployment benefits). The IG has testified that one of the three biggest challenges his office faces in overseeing the UI program is a "lack of ongoing, timely, and complete access to UI claimant data and wage records" from state workforce agencies.[29]

- *Update program reporting requirements.*

Data reporting issues confounded efforts to understand the number of people collecting key unemployment benefits early in the pandemic. As GAO concluded in November 2020, "Without an accurate accounting of the number of individuals who are relying on UI and PUA benefits in as close to real-time as possible, policy makers may be challenged to respond to the crisis at hand."[30] Instead of relying on users to divine the meaning of its data, DOL should either more clearly label its weekly initial claims reports (such as for "weeks of benefits claimed") or provide information that reflects the number of individuals claiming benefits—as the media regularly and inaccurately reported during the pandemic.

New emergency programs have their own reporting problems. Due to the PUA program's operational intensity and technology challenges, it is perhaps understandable that states did not

[28] Allan Smith, "Handful of GOP senators threaten to delay Senate coronavirus bill over unemployment payments," NBC News, March 25, 2020, https://www.nbcnews.com/politics/congress/handful-gop-senators-threaten-delay-senate-coronavirus-bill-over-drafting-n1168766

[29] U.S. Department of Labor Office of Inspector General Congressional Testimony, February 8, 2023, https://waysandmeans.house.gov/wp-content/uploads/2023/02/DOL-OIG-IG-Turner-Written-Testimony-HWM-_Final-02062023.pdf

[30] Government Accountability Office, "Urgent Actions Needed to Better Ensure an Effective Federal Response," November 2020, https://www.gao.gov/assets/gao-21-191.pdf

prioritize reporting early in the pandemic. However, the PUA data as reported in the ETA 902-P form shows that some states never fixed that gap. There are very real technical, environmental, and resource obstacles to accurate reporting in temporary programs, but there is also a cost to not getting any data. Limited or inaccurate data can limit the capacity of policymakers, program stakeholders, and state leaders to define success, identify problems, and make needed program changes.

On the technology front, states could be asked to report on fraud posture and defenses across a range of use cases. Regardless of solutions chosen, states should be able to demonstrate they have or are working toward an adaptive, flexible and responsive fraud detection and prevention posture.

Conclusion

Suggesting that benefit timeliness and benefit accuracy must be opposing goals is a false dichotomy. Benefit timeliness for eligible claimants is often most possible when fraud attacks are identified and prevented. Eligible claimants and taxpayers pay a steep price when policymakers do not take fraud prevention, detection, investigation and/or prosecution as seriously as the circumstances warrant. Learning the lessons of the pandemic unemployment insurance fraud experience is, at its core, defense of the unemployment insurance program's original intent: to provide a temporary partial income replacement safety net for workers who have lost work by no fault of their own. History does not need to repeat itself; all stakeholders have a vested interest in ensuring that fraud detection and prevention is an integral, permanent part of the program's mission.

Chairman SCHWEIKERT. Thank you, Ms. Simon.
Ms. Shea.

STATEMENT OF REBECCA SHEA, DIRECTOR OF AUDITS, FORENSIC AUDITS AND INVESTIGATIVE SERVICES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. SHEA. Good morning, Chairmen Smith, Schweikert, and Ranking Member Pascrell, and members of the subcommittee. Thank you for inviting me to discuss some of GAO's resources and recommended actions to better prevent fraud in normal operations after the unprecedented levels of fraud in COVID relief programs.

GAO's goal in general, and my goal in particular as a director in our forensic audit group, is to encourage agencies to prevent fraud in order to avoid the very costly pay-and-chase approach. The importance of prevention is the cornerstone of GAO's fraud risk framework. Requirements have been in place for many years for agencies to manage fraud risk. But, as GAO's comptroller general testified earlier this year, agencies' lag in implementing these requirements led to significant fraud in COVID programs.

Yes, agencies across the Federal Government acted quickly to stand up new programs and greatly scale up existing programs to combat the effects of the pandemic. And yes, that made for an unusually attractive target to fraudsters. But the nature of COVID relief schemes was not dissimilar from fraud schemes that occurred in years prior.

Some schemes were simple and benefited a simple—a single fraudster, like a case where an individual received a quarter million dollars from the Coronavirus Food Assistance Program for claimed loss of livestock at a commercial farming operation, despite not owning or operating a farm. Others used technology or brought others along to scale up the impact of the fraud, like a case where the owner of a tax preparation business recruited people to prepare fraudulent tax returns and COVID EIDL loan applications. She charged her clients up to 50 percent of the fraudulent proceeds and paid her employees a flat fee for each application that received funding, and she also claimed fraudulent EIDL, PPP, and unemployment benefits for herself.

Regardless of scale, misrepresentations of eligibility and identity are primarily at the core of these schemes. Had agencies been better prepared to prevent and detect identity and eligibility representations in normal operations, they would have been better prepared for the emergency, which leads us to the question of why agencies weren't prepared and what is needed to get them there.

Based on my audit experience, I would put the root causes for this in two buckets: mindset and direction. The mindset issue I have seen is that program managers often don't think fraud is a problem, at least not in their programs, or they don't think fraud is their problem, particularly when the program is administered through grants, contracts, or other third parties. And if agencies don't think there is a problem, or that it is theirs to manage, they aren't going to spend time and resources on it. The unprecedented scope and scale of COVID relief fraud has put a dent in that mindset, but we need sustained focus on accountability to eliminate

that mindset once and for all, and that is where GAO resources and congressional action can provide direction.

In addition to our audits and recommendations to address specific fraud vulnerabilities, GAO has developed resources like our conceptual fraud model, our fraud risk framework, our anti-fraud resource, and, most recently, our framework for managing improper payments, all of which provide a roadmap for fraud prevention. Providing this direction was a key driver for developing our conceptual fraud model that lays out the who, what, how, why, and where of fraud schemes so agencies can better understand what fraud looks like and how it happens in order to respond to those vulnerabilities.

GAO has also suggested actions Congress can take, including reinstating requirements for agencies to report on their progress with fraud prevention, making permanent the data analytics function in the oversight community, and making permanent Treasury's access to Social Security's full death data to help prevent payments to deceased individuals.

In addition to these efforts, GAO has work underway to identify possible incentives for fraud risk management such as funding options, ways to measure prevention activities, and enhance data sharing and analytic programs.

Unfortunately, not everyone's moral compass points due north. Fraud will happen, and bad actors will be creative in finding vulnerabilities and exploiting opportunities for their personal gain. But with a better understanding of how fraud happens, by leveraging available resources to prevent fraud, and by taking actions GAO has recommended to agencies and to Congress, the Federal Government as a whole will be better positioned to prevent fraud in any environment.

I thank you for this opportunity and look forward to your questions.

[The statement of Ms. Shea follows:]

United States Government Accountability Office

Testimony

Before the Subcommittee on Oversight, Committee on Ways and Means, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, October 19, 2023

COVID-19

Key Elements of Fraud Schemes and Actions to Better Prevent Fraud

Statement of Rebecca Shea, Director, Forensic Audits and Investigative Service

GAO-24-107122

GAO Highlights

Highlights of GAO-24-107122, a testimony before the Subcommittee on Oversight, Committee on Ways and Means, House of Representatives

Why GAO Did This Study

Since March 2020, Congress and the Administration have provided trillions of dollars in COVID-19 relief funding to help the nation respond to and recover from the pandemic. Agencies across the federal government acted quickly to stand up new programs and greatly scale up existing programs.

The unprecedented demand for benefits and the need to quickly implement or expand programs increased the risk of fraud during the pandemic. There have also been cases of funds paid to those who sought to defraud the government. For example, from March 2020 through June 2023, at least 1,399 individuals or entities were found guilty or liable for fraud-related charges in cases involving federal COVID-19 relief programs.

Managing fraud risk is the responsibility of program managers and includes assessing the potential for fraud and implementing strategies to appropriately mitigate related fraud risks. Better understanding the nature of federal fraud schemes and the resources available to combat them can enhance agency efforts to prevent, detect, and respond to fraud risk during normal operations and emergencies.

This testimony discusses (1) key elements of federal fraud schemes and examples of schemes involving COVID-19 relief funds and (2) actions agencies and Congress can take to better prevent fraud during normal operations and emergencies.

GAO reviewed its prior COVID-19 findings and recommendations on internal controls and fraud risk management practices.

View GAO-24-107122. For more information, contact Rebecca Shea at (202) 512-6722 or shear@gao.gov.

October 19, 2023

COVID-19

Key Elements of Fraud Schemes and Actions to Better Prevent Fraud

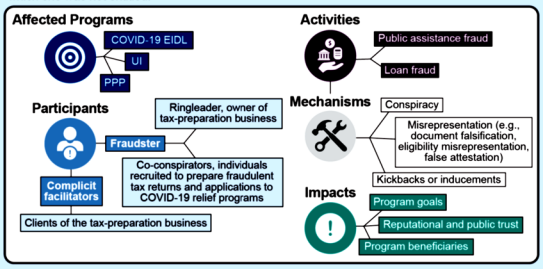
What GAO Found

Most COVID-19 relief funds went to the intended recipients in the intended amounts. In other instances, significant funds went to those who engaged in fraud schemes. Federal fraud schemes consist of five key elements: (1) affected program, (2) participants, (3) types of fraud activities, (4) mechanisms to execute fraudulent activities, and (5) impacts. These elements represent the highest-level components in GAO's Conceptual Fraud Model. The model provides a common language and structure for describing fraud schemes—including those affecting COVID-19 relief programs—to support agency efforts to combat fraud.

Key Elements of an Example of a Fraud Scheme Involving Multiple COVID-19 Relief Programs

Four defendants were sentenced for conspiracy to defraud several COVID-19 relief programs.

Through her tax-preparation business, the ringleader recruited at least five people to prepare fraudulent tax returns and applications to COVID-19 relief programs for clients. She charged her clients up to 50 percent of the fraudulent COVID-19 Economic Injury Disaster Loan (COVID-19 EIDL) program proceeds, paying her employees a flat fee for each fraudulent application that received funding. She also submitted fraudulent COVID-19 EIDL applications in her own name. In addition, she defrauded the Paycheck Protection Program (PPP) by obtaining a fraudulent PPP loan of $3,548. Finally, she also claimed more than $33,000 in unemployment insurance (UI) payments to which she was not entitled.



Source: GAO analysis of court documentation; GAO (icons). | GAO-24-107122

Federal agencies did not strategically manage fraud risks and were not adequately prepared to prevent fraud when the pandemic began. While eliminating all fraud is not a realistic goal, resources and requirements exist to support strategic fraud risk management. For example, GAO's Fraud Risk Framework and Antifraud Resource provide leading practices and interactive tools, respectively, to help agencies combat fraud. GAO's 142 recommendations to agencies to align their efforts with fraud risk management leading practices also provide a roadmap for action. GAO has also suggested actions Congress can take, such as reinstating agencies' reporting on fraud risk management and enhancing data analytic capabilities. These congressional actions and agencies' use of GAO resources to strategically manage fraud risk would position them to better prevent fraud in both normal operations and in emergencies.

Chairman Schweikert, Ranking Member Pascrell, and Members of the Subcommittee:

I appreciate the opportunity to discuss key elements of fraud schemes involving COVID-19 relief programs, as well as what can be done to prevent fraud in the future.[1]

Since March 2020, Congress and the Administration have provided trillions of dollars in COVID-19 relief funding to help the nation respond to and recover from the pandemic. Agencies across the federal government acted quickly to stand up new programs and greatly scale up existing programs. Federal COVID-19 relief funds were distributed broadly to tribal, state, local, and territorial governments; businesses; and individuals to combat the effects of the pandemic on the public health system as well as on the economy.

Most of these funds went to the intended recipients in the intended amounts, providing needed assistance. However, in other instances, funds were paid to those who sought to defraud the government. For example, from March 2020 through June 2023, at least 1,399 individuals or entities were found guilty or liable for fraud-related charges in cases involving federal COVID-19 relief programs.[2] More are facing charges. Through June 30, 2023, federal charges were pending against at least 599 individuals or entities for attempting to defraud COVID-19 relief programs. Cases that reach the prosecution stage in the fraud identification lifecycle represent a fraction of the instances of fraud or all possible fraud cases.

The unprecedented demand for benefits and the need to quickly implement or expand programs increased the risk of fraud during the pandemic. Managing fraud risk is the responsibility of federal program managers and includes assessing the potential for fraud and implementing strategies to appropriately mitigate related risks. Better understanding the nature of federal fraud schemes and the resources

[1]Fraud involves obtaining something of value through willful misrepresentation.

[2]We consider cases closed upon acceptance of guilty pleas, guilty verdicts at trial, or findings of liability based on our analysis of Department of Justice (DOJ) public statements and court documentation. The federal government may enforce laws through civil or criminal action. Such action may be resolved through a trial, a permanent injunction, a civil settlement, or a guilty plea. Our analysis is limited to the cases we identified from public sources and may not include all criminal and civil cases charged by DOJ as of June 30, 2023.

available to combat them can enhance agency efforts to prevent, detect, and respond to fraud risk in normal operations and emergencies.

My comments today summarize key findings from our Conceptual Fraud Model, Antifraud Resource, and fraud-related COVID-19 work. Specifically, I will discuss the following:

1. Key elements of federal fraud schemes and examples of schemes involving COVID-19 relief funds and
2. Actions federal agencies and Congress can take to better prevent fraud during normal operations and emergencies.

In preparing this testimony, we reviewed findings from our prior work on internal controls and fraud risk management practices in COVID-19 relief programs. Given the government-wide scope of this work, we undertook a variety of methodologies. These methodologies include examining federal laws and agency documents, guidance, processes, and procedures. We also interviewed federal and state officials. More detailed information on the objectives, scope, and methodology that this statement is based on can be found in the individual reports from which we obtained this information.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

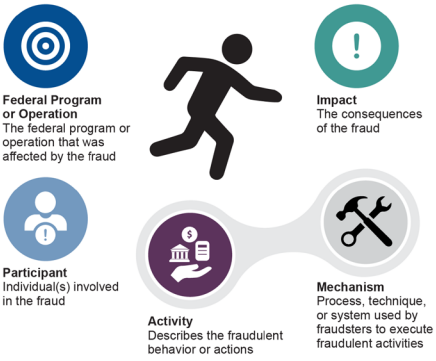
Federal Fraud Schemes Include Five Key Elements

To better understand and assess the nature of known fraud—both financial and nonfinancial—affecting federal programs and operations, we developed a Conceptual Fraud Model (fraud model).[3] While we developed and released the fraud model during the COVID-19 pandemic, it is applicable across federal programs during normal operations and emergencies.

[3]The Conceptual Fraud Model is organized as an "ontology." An ontology is an explicit description of categories in a subject area and their characteristics, as well as the relationships among them. To develop our fraud model, we collected, reviewed, and analyzed multiple sources of information, including over 200 adjudicated federal criminal and civil fraud cases to validate and refine the fraud model.

The fraud model identifies five key elements of fraud schemes affecting federal programs and operations. These include (1) the affected program or operation, (2) participants, (3) types of fraud activities, (4) mechanisms used to execute the activities, and (5) impacts of the fraud scheme, as depicted in figure 1. The full model demonstrates the complexity of fraud relationships that affect the federal government, such as how fraudsters use mechanisms to execute fraud activities and their impacts on individuals and the government.

Figure 1: Five Key Elements of Fraud Schemes Affecting the Federal Government



Source: Antifraud Resource (gaoinnovations.gov). | GAO-24-107122

The five key elements reflect the highest-level components of the model. Systematically organized subcomponents of the full model are available for download and exploration from GAO's Antifraud Resource website.[4] The model was developed to help promote a common understanding of fraud that affects the federal government. The model can also be used to enhance data analytics by providing a common framework and

[4]GAO, "The GAO Antifraud Resource" (Washington, D.C.: Jan. 10, 2022), accessed Oct. 14, 2023, https://gaoinnovations.gov/antifraud_resource/.

vocabulary to describe and classify fraud affecting the federal government.

Element 1: Affected Programs or Operations

The federal government collects and spends funds to support a broad range of programmatic and operational objectives. These include objectives related to education, health care, research, infrastructure, economic development, and national defense. This broad range of activities, as well as the scope of those expenditures, makes government functions a target for fraudsters. When federal programs or operations are targeted by fraud, it also exposes federal employees and stakeholders to other risks, such as program integrity challenges and organizational reputational risks.

Multiple Affected Programs in a Fraud Scheme Involving COVID-19 Economic Injury Disaster Loan (COVID-19 EIDL) Program, Paycheck Protection Program (PPP), and Unemployment Insurance (UI)

Participants

Four defendants were sentenced for conspiracy to defraud several COVID-19 relief programs. The ringleader was sentenced to 4 years in federal prison and ordered to pay $38,756 in restitution and a fine of $20,000.

Fraud scheme

Through her tax-preparation business, the ringleader recruited at least five people to prepare fraudulent tax returns and applications to COVID-19 relief programs for clients. She charged her clients up to 50 percent of the fraudulent COVID-19 EIDL proceeds, paying her employees a flat fee for each fraudulent application that received funding. She also submitted fraudulent COVID-19 EIDL applications in her own name. She defrauded PPP by obtaining a fraudulent PPP loan of $3,548. Finally, she also claimed more than $33,000 in UI payments to which she was not entitled.

Impacts

Instead of going to small businesses in need or individuals facing unemployment during the pandemic, the defendants redirected those funds to their own purposes.

Source: GAO analysis of court documentation. | GAO-24-107122.

Affected COVID-19 relief programs. A variety of COVID-19 relief programs were targets in fraud schemes, with some schemes involving multiple programs. The majority of the 1,399 individuals or entities found guilty or liable had charges related to the Small Business Administration's (SBA) Paycheck Protection Program (PPP) or COVID-19 Economic Injury Disaster Loan (COVID-19 EIDL) program or the Department of Labor's (DOL) unemployment insurance (UI) programs. However, other targeted programs include

- Department of the Treasury and the Internal Revenue Service's economic impact payments;
- Treasury's Emergency Rental Assistance program and Coronavirus Relief Fund;
- Department of Agriculture's federal child nutrition programs and Coronavirus Food Assistance Program;
- Department of Education's Higher Education Emergency Relief Fund;
- Department of Health and Human Services' Health Resources and Services Administration's COVID-19 Uninsured Program and Provider Relief Fund, and the Centers for Medicare & Medicaid Services' Accelerated and Advance Payment Program; and
- Federal Reserve's Main Street Lending Program.

Some schemes involved multiple COVID-19 relief program targets, such as one scheme to fraudulently receive funds from three programs—COVID-19 EIDL, PPP, and UI (see sidebar).

Element 2: Participants

Fraudster Operating from Within to Defraud the Unemployment Insurance (UI) Program

Participants

A contract employee for a state workforce agency was sentenced to almost 5 years in prison and ordered to pay around $4 million in restitution for wire fraud.

Fraud scheme

The employee was responsible for reviewing, processing, and verifying the legitimacy of CARES Act UI claims. Using insider access, the employee disbursed to personal accounts over $2 million in federal and state funds intended for unemployment assistance.

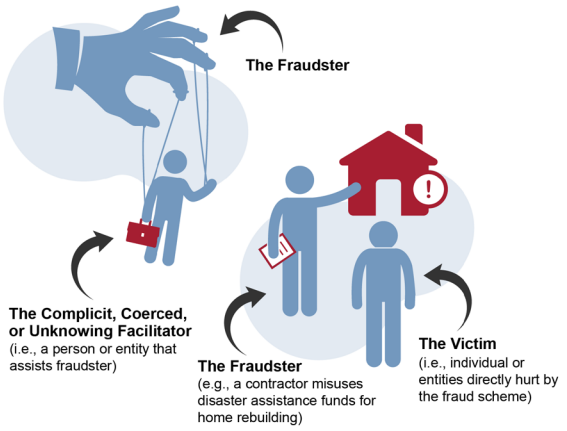
Impacts

Rather than ensuring unemployment funds went to those in need, the employee used her position to fraudulently obtain funds to purchase high-end handbags and other luxury goods.

Source: GAO analysis of court documentation. | GAO-24-107122.

Every fraud scheme has at least one fraudster. The fraudster(s) may attack from within or outside the affected federal program or operation (see sidebar). A fraudster may be aided by one or more facilitators, who provide assistance to the fraudster. Some facilitators knowingly participate in fraud schemes by being complicit or coerced. Other facilitators may unknowingly participate in fraud schemes, such as by providing personal identifying information (PII) for one purpose, but that PII is then used without their knowledge to further a fraud scheme. Fraud scheme participants also include victims—participants directly hurt by the scheme. See figure 2 for the different types of participants associated with fraud schemes.

Figure 2: Types of Participants Associated with Fraud Schemes



Source: Antifraud Resource (gaoinnovations.gov). | GAO-24-107122

Complicit Facilitators in an Economic Impact Payments (EIP) Fraud Scheme

Participants

Two members of a family were sentenced to federal prison, and a third to probation, for their roles in a $530,293 scheme to file false tax returns and steal EIPs sent to others. In addition, the three were ordered to pay $150,894 in restitution.

Fraud scheme

Acting as tax preparers, the family recruited foreign individuals who had spent time in the United States to file fraudulent returns for education and other credits. To hide the scheme, the family enlisted others to open U.S. bank accounts to deposit the refunds, ultimately opening 68 accounts across 16 banks in the names of 14 different individuals. When EIPs were sent to qualifying individuals with bank accounts on file, hundreds of payments were made into the accounts under their control based on the false returns they had filed.

Impacts

While the EIP was intended to support families in need, this family stole emergency support funds to use on personal expenses and to buy real estate. Approximately $380,000 of stolen funds were recovered, primarily through sales of the ill-gotten property.

Source: GAO analysis of court documentation. | GAO-24-107122.

Participants in COVID-19 relief program fraud schemes. COVID-19 relief program fraud schemes included participants within and outside the affected federal programs. These fraud schemes also involved participants acting alone or in concert with others, involving domestic and international actors, and leveraging complicit and unknowing facilitators (see sidebar). COVID-19 relief program fraud schemes involved a wide variety of victims.

Complicit facilitator – Our prior work illustrated schemes involving complicit individuals who facilitated PPP and COVID-19 EIDL fraud for others, sometimes in return for a kickback payment.[5] For example, cases involving registered agents charged with fraudulently obtaining PPP and COVID-19 EIDL funds illustrate the role of complicit facilitators.[6] As professional service providers, registered agents have access to business information, including shell companies, and business formation functions. In our review of fraud in SBA pandemic programs, we found examples where registered agents took advantage of their role, for themselves and others, to obtain about $197.6 million in PPP and COVID-19 EIDL funds.

In a scheme that stole at least $180,000 in UI benefits, a fraudster collaborated with prison inmates to submit fraudulent applications.[7] The fraudster pleaded guilty to charges including conspiracy to defraud the United States and was sentenced to 2.8 years in prison. The fraudster was also ordered to pay $142,069 in restitution.

Victims – Our prior work also illustrated schemes involving victims such as identity theft victims who were directly hurt by a fraud scheme.[8] For example, a fraudster used stolen identities or PII from victims to apply for UI benefits. The fraudster participated in a scheme to submit fraudulent claims to multiple states using fake identification cards. The fraudster also created financial accounts in the victims' names to receive funds. The fraudster pleaded guilty to charges including identity theft and was

[5]GAO, *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs*, GAO-23-105331 (Washington, D.C.: May 18, 2023).

[6]Registered agents are persons or entities authorized to accept service of process or other important legal or tax documents on behalf of a business and are frequently involved in business formation.

[7]See GAO, *Unemployment Insurance: DOL Needs to Address Substantial Pandemic UI Fraud and Reduce Persistent Risks*, GAO-23-106586 (Washington, D.C.: Feb. 8, 2023).

[8]GAO-23-106586.

sentenced to 4 years in prison. The fraudster was also ordered to pay $299,500 in restitution.

Element 3: Types of Fraud Activities

The activity describes the type of fraudulent behavior or actions. All fraud schemes involve one or more types of fraud, such as tax fraud, health care fraud, corporate fraud, and identity fraud. Fraudulent activities can occur in federal programs and operations due to weak internal controls.

Activities can be financial or nonfinancial. Nonfinancial activities can include trying to achieve prestige, circumvent regulations or rules, or achieve a different status. For example, educational institutions at all levels may inflate grades to show adherence to standardization goals. Corporations may alter data to show they are in compliance with environmental or workplace safety rules. Individuals may falsify documents to gain citizenship or assume another identity. Fraud activities are accomplished through the use of mechanisms, another key element of fraud schemes.

COVID-19 relief program fraud activities. The types of fraud activities present in COVID-19 relief program schemes varied, with multiple activities often employed in a single scheme.

Beneficiary fraud – Beneficiary fraud—an activity that uses willful misrepresentation in order to improperly obtain a benefit for a beneficiary or at their expense—was a type of activity seen in COVID-19 relief program schemes (see sidebar).

Identity fraud – Identity fraud—an activity that uses the theft of personal information in order to fraudulently obtain benefits—was a key fraud activity among COVID-19 relief program schemes. Our prior work illustrated schemes involving use of various types of identity fraud to obtain PPP and COVID-19 EIDL funds. Identity fraud can be accomplished through mechanisms such as theft of personally identifiable and business information or the abuse of shell companies.[9] For example, in one case of identity fraud, the fraudster used stolen personal information (along with shell companies and false attestation) to obtain PPP funds. The same fraudster also engaged in synthetic identity fraud by fabricating an identity using fictitious information in combination with stolen information such as a Social Security number.

Beneficiary Fraud Scheme to Obtain Coronavirus Food Assistance Program (CFAP) Funds

Participants

An individual was sentenced to 2.5 years in prison and around $250,000 in restitution for making a false claim to CFAP.

Fraud scheme

The individual claimed loss of livestock at a commercial farming operation, despite not owning or operating a farming operation. The individual also submitted a fraudulent IRS Form 7200 to request an advance payment of employer credits under the Families First Coronavirus Response Act.

Impacts

In total, the individual attempted to obtain over $1.5 million in COVID-19 relief funding.

Source: GAO analysis of court documentation. | GAO-24-107122.

[9]GAO-23-105331.

Element 4: Mechanisms

The mechanism is a process, technique, or system used by fraudsters to execute fraudulent activities. A mechanism can be an individual action or a group of actions working in concert, such as:

- Misrepresentation
- Cybercrime
- Coercion
- Document falsification
- Data breach
- Social engineering

Multiple Mechanisms Used in a Federal Child Nutrition Program Fraud Scheme

Participants

Three individuals associated with a nonprofit organization pleaded guilty to their roles in a $250 million scheme to defraud a federal child nutrition program. Over 40 individuals have been charged in the scheme.

Fraud scheme

Through the abuse of shell companies, bribes, kickbacks, and fake invoicing, individuals claimed reimbursement for purportedly serving meals to hundreds or thousands of children a day. In total, the individuals claimed to have served over 1.3 million meals from December 2020 through June 2021, and received over $3 million in reimbursement.

Impacts

Rather than using funds to feed children in need, the individuals used the proceeds for their personal purposes.

Source: GAO analysis of court documentation. | GAO-24-107122.

Fraudsters may use considerable skill and innovation when employing mechanisms. Fraud mechanisms are used to execute both financial and nonfinancial activities. For example, contract fraud (type of fraud activity) often occurs for financial gain and may use mechanisms that assist the fraudster before or after the contract is awarded. Contract fraud mechanisms can include actions like "bid-splitting," billing manipulation, and fictitious vendors.

COVID-19 relief program fraud mechanisms. Multiple and various mechanisms were used in COVID-19 relief program fraud schemes (see sidebar for a scheme using various mechanisms). The mechanisms used in a fraud scheme have a close relationship to internal controls. For example, mechanisms of misrepresentation, such as document manipulation, false declarations, and fictitious entities leave agencies open to significant fraud risk when they rely on self-certification as an internal control for fraud prevention. Confirming the eligibility and identity of individuals receiving payments, such as by confirming wage information or verifying identity through data and other checks, are key controls to prevent fraud schemes that rely on such mechanisms. We found that federal and state agencies relied on self-attestation or self-certification for individuals to verify their eligibility or identity to receive assistance from some COVID-19 relief programs in order to disburse funds quickly to those in need.[10]

[10]For example, one of the temporary UI programs—the Pandemic Unemployment Assistance (PUA) program—initially allowed applicants to self-certify their eligibility and did not require them to provide any documentation of self-employment or prior income. In addition, the CARES Act initially restricted SBA from obtaining federal tax return transcripts as part of the COVID-19 EIDL application process. As a result, SBA relied on self-certification when processing loan and advance applications. The

Document falsification – Our prior work illustrated schemes involving falsification of documents, such as tax forms, payroll documentation, and bank statements to obtain PPP and COVID-19 EIDL funds.[11] Additionally, false information about other elements of PPP and COVID-19 EIDL loan applications, such as employee counts and payroll amounts, were prevalent in DOJ cases as well. For example, we found that more than half of the PPP and COVID-19 EIDL cases we reviewed involved falsification of payroll documentation or bank statements or allegations of tax document falsification, showing that tax forms may have been commonly forged or altered.

Element 5: Impacts

The impact of a fraud scheme describes the outcomes that resulted from the fraud. One fraud scheme could have a narrow impact on a sole individual, while another could affect multiple individuals or groups. Impacts can be financial, nonfinancial, or both. Although sometimes overlooked, nonfinancial impacts are equally as important because they can threaten society, such as by affecting public health or national security.

In addition to the public's loss of trust, other effects of fraud at the federal level may include:

- Economic impacts
- Public health and safety
- National security implications
- Program impacts (i.e., the ability of a program to achieve its mission)
- Reputational impact
- Impacts on the fraudster (if caught or detected)

Consolidated Appropriations Act, 2021, enacted in December 2020, addressed both of these situations.

[11]GAO-23-105331.

Impacts on Small Businesses from Fraud in Paycheck Protection Program (PPP)

Participants

An individual was sentenced to more than 11 years in prison and ordered to pay over $17 million in restitution in connection with his fraudulent scheme to obtain approximately $24.6 million in PPP loans.

Fraud scheme

The individual submitted 15 fraudulent applications to eight different lenders for purported businesses he owned or controlled, claiming these businesses had numerous employees and hundreds of thousands of dollars in payroll expenses when, in fact, no business had employees or paid wages consistent with the amounts claimed. The individual received over $17 million in PPP loan funds.

Impacts

As COVID-19 devastated companies around the nation, this individual diverted millions of dollars from the relief fund that could have helped them. He used the funds to purchase multiple homes, pay off mortgages on other homes, and buy a fleet of luxury cars. He also sent millions of dollars in PPP proceeds in international money transfers.

Source: GAO analysis of court documentation. | GAO-24-107122

Impacts of COVID-19 relief program fraud schemes. The impacts of COVID-19 relief program fraud schemes are widespread and will continue to unfold for years to come. The number of individuals or entities facing fraud-related charges will likely continue to increase, as these cases take time to develop. Also, one of the many challenges in determining the full extent and impact of fraud is its deceptive nature. Programs can experience fraud that is never identified and the related losses and impacts are difficult to determine. Some of the impacts of COVID-19 relief program fraud schemes were direct, such as the loss of taxpayer dollars. Other impacts were less direct, such as from the loss of access to needed funds because they were diverted by fraudsters (see sidebar).

Program and reputation impact – The impacts of fraud go beyond financial losses. Public perception of widespread fraud in pandemic relief programs can erode trust in government—including confidence in the government's ability to manage taxpayer dollars, to prevent fraud, and to pursue justice. According to DOJ officials, instances of fraud can normalize additional fraudulent behavior, which increases cynicism among the public. A high incidence of fraud can lead to public perception that pandemic relief funds are easy to obtain fraudulently and make the government a target for further exploitation.

Impacts of Identity Theft from a COVID-19 Economic Injury Disaster Loan Program (COVID-19 EIDL) Advance Fraud Scheme

Participants

Two individuals were sentenced to 121 and 66 months in federal prison, respectively, and ordered to forfeit $680,710 and pay more than $3.7 million in monetary penalties for their roles in a COVID-19 EIDL fraud scheme.

Fraud scheme

The duo operated a telemarketing scheme where, in exchange for a fee, they took personal identifying information (PII) from victims and promised to file an application for an agricultural grant. Instead, they filed fraudulent COVID-19 EIDL applications using the victims' PII. They received $1.56 million in COVID-19 EIDL Advances and attempted to receive an additional $1.44 million. They also used a credit and debit card processing service to charge third parties, from which they obtained at least $700,000 in fees.

Impacts

The duo diverted needed funds from legitimate businesses and used individuals' PII without their consent. They transferred stolen funds to their personal bank account.

Source: GAO analysis of court documentation. | GAO-24-107122

Impacts on individuals – Identity theft inflicts damage to victims' financial and emotional health. According to DOJ, victims of identity theft have had their bank accounts wiped out, had their credit histories ruined, and had jobs and valuable possessions taken away. In COVID-19 relief program fraud cases, according to DOJ officials, identity theft affects victims through (1) negative impacts on credit, (2) denial of entitlements and other benefits (e.g., unemployment benefits) because of prior claims filed using victims' identities, (3) susceptibility to other types of fraud, and (4) time and effort spent rectifying issues related to identity theft. Identity theft can also affect victims' physical and psychological health. Victims may experience anxiety, sleeplessness, and depression, among other symptoms. According to DOJ, the emotional trauma associated with identity theft can be as devastating as many violent offenses. (See sidebar for impacts of identity theft.)

Impacts on fraudster – Fraud also impacts those perpetrating the scheme. Of the individuals found guilty, at least 1,051 had been sentenced as of June 30, 2023. Sentences for these cases vary. The range in length of prison sentencing varies, in part based on other relevant factors such as prior convictions, and whether there were other

charges in addition to COVID-19 related fraud.[12] For example, in one case of UI fraud, an individual was sentenced to 1 year of probation and ordered to pay a $2,000 fine and over $16,000 in restitution. In another case, an individual who pleaded guilty to PPP fraud was sentenced to over 17 years in prison and 5 years supervised release and ordered to pay nearly $4.5 million in restitution.

Agencies and Congress Can Take Actions Now to Better Prevent Fraud

Federal agencies did not strategically manage fraud risks and were not adequately prepared to prevent fraud when the pandemic began. We recognize that eliminating all fraud and fraud risk is not a realistic goal. However, a variety of resources and requirements for fraud risk management were in place well before the pandemic. Had agencies already been strategically managing their fraud risks, they would have been better positioned to identify and respond to the heightened risks that emerged during the pandemic. Agencies have the opportunity to learn from the experiences during the pandemic and to ensure that they are strategically managing their fraud risks. Doing so by leveraging available resources and adhering to requirements will enable them to carry out their missions and better protect taxpayer dollars from fraud during normal operations and prepare them to face the next emergency.

One such resource is *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework), issued in July 2015.[13] This framework provides a comprehensive set of key components and leading practices to help agency managers combat fraud in a strategic, risk-based way. The Payment Integrity Information Act of 2019 requires that the guidelines for federal agencies established by the Office of Management and Budget

[12]Courts refer to the *United States Sentencing Commission Guidelines Manual* (Guidelines) to determine the particular sentence in each individual case. Under 28 U.S.C. § 994, the Guidelines should reflect a variety of factors and considerations to determine an appropriate sentence. The Guidelines set a base offense level and then add or subtract levels due to aggravating or mitigating circumstances, such as the dollar amount of the loss caused by offense, as well as the defendant's criminal history, ultimately arriving at a suggested sentencing range. Additionally, many of the defendants we reviewed were convicted on additional charges beyond fraud against COVID-19 relief programs, which would impact the length of their sentences.

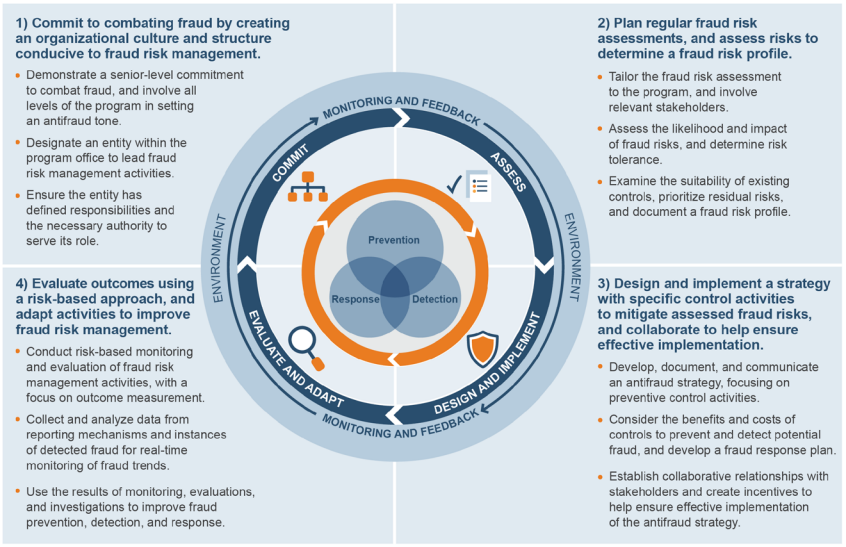
[13]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015).

(OMB)—which incorporate the leading practices from the Fraud Risk Framework—remain in effect.[14]

As depicted in figure 3, the Fraud Risk Framework describes leading practices for managing fraud risk and includes four components: commit, assess, design and implement, and evaluate and adapt. These leading practices are applicable during normal operations, as well as during emergencies.

[14]Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131 - 132 (2020), codified at 31 U.S.C. § 3357. The act requires these guidelines to remain in effect, subject to modification by OMB as necessary, and in consultation with GAO. The Fraud Reduction and Data Analytics Act of 2015 required OMB to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement anti-fraud control activities. The act further required OMB to incorporate the leading practices from the Fraud Risk Framework in the guidelines. Pub. L. No. 114-186, 130 Stat. 546 (2016). In October 2022, OMB issued a Controller Alert reminding agencies that consistent with the guidelines contained in OMB Circular A-123, which are required by Section 3357 of the Payment Integrity Information Act of 2019, Pub. L. No. 116-117, they must establish financial and administrative controls to identify and assess fraud risks. In addition, OMB reminded agencies that they should adhere to the leading practices in GAO's Fraud Risk Framework as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risks. OMB, CA-23-03, *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk* (Oct. 17, 2022).

Figure 3: The Four Components of the Fraud Risk Framework and Selected Leading Practices



Source: GAO (information and icons). | GAO-24-107122

Another resource is the Bureau of the Fiscal Service's Antifraud Playbook that provides a how-to guide for implementing the Fraud Risk Framework's leading practices.[15] The Playbook consists of a four-phased approach—aligned with the four components of the Fraud Risk Framework—and 16 best-practice plays for combatting fraud.

We expressed concern in March 2022 about the pace and extent to which agencies have implemented controls to prevent, detect, and respond to

[15]Bureau of the Fiscal Service, *Program Integrity: The Antifraud Playbook* (Oct. 17, 2018), accessed Oct. 14, 2023, https://www.cfo.gov/assets/files/Interactive-Treasury-Playbook.pdf.

fraud in a manner consistent with leading practices since the Fraud Reduction and Data Analytics Act's enactment in 2016.[16]

In April 2023, we issued a retrospective review of GAO reports on agencies' efforts to manage fraud risks in alignment with leading practices from the Fraud Risk Framework.[17] Since we issued the framework in 2015, we have issued over 70 reports with recommendations to agencies to align their efforts with leading practices. Among the 142 recommendations from these reports issued from July 2015 through December 2022, agencies needed to take additional action to fully address 74 of these recommendations, as of January 2023.[18] Fully addressing these recommendations can help ensure that federal managers safeguard public resources, including while providing needed relief during emergencies.

Our review highlighted five areas in which federal agencies need to take additional actions to help ensure that they are effectively managing fraud risks consistent with leading practices, as shown in figure 4.

Figure 4: Federal Agencies Need to Improve Fraud Risk Management Efforts in Five Areas

Source: GAO (information and icons). | GAO-24-107122

[16]GAO, *Emergency Relief Funds: Significant Improvements Are Needed to Ensure Transparency and Accountability for COVID-19 and Beyond*, GAO-22-105715 (Washington, D.C.: Mar. 17, 2022).

[17]GAO, *Fraud Risk Management: Key Areas for Federal Agency and Congressional* Action, GAO-23-106567 (Washington, D.C.: Apr. 13, 2023).

[18]As of January 2023, of the 142 recommendations, 67 were closed as implemented, one was closed as not implemented, 11 were open but had been partially addressed, and 63 were open and had not been addressed. We follow up on recommendations we have made and update the status at least once per year. Experience has shown that it takes time for some recommendations to be implemented. Of the 142 recommendations, 21 were made on or after January 1, 2022, and 19 of the 21 remained open as of January 2023. Some recommendations relate to more than one area. For example, we made a recommendation to the Department of Health and Human Service's Administration for Children and Families to conduct a fraud risk assessment to provide a basis for the documentation and development of an antifraud strategy for the Child Care and Development Fund.

In addition to the Fraud Risk Framework, we have developed other resources—specifically our web-based Antifraud Resource and *A Framework for Managing Improper Payments in Emergency Assistance Programs* (Managing Improper Payments Framework)—to help agencies combat fraud and improve payment integrity.[19] These resources can help agencies better understand and combat the causes and impacts of fraud.

Antifraud Resource. Our prior work found that agencies have had challenges effectively assessing and managing their fraud risks and federal managers may not fully understand how fraud affects their programs. GAO created the online Antifraud Resource to help federal officials and the public better understand and combat federal fraud. The Antifraud Resource is based on the previously discussed conceptual fraud model and provides insight on fraud schemes that affect the federal government, their underlying concepts, and how to combat such fraud. Figure 5 references the online location of this antifraud resource.[20]

Figure 5: Reference to GAO's Antifraud Resource

Source: GAO and Production Perig/stock.adobe.com (image). | GAO-24-107122

Managing Improper Payments Framework. When the federal government provides emergency assistance, the risk of improper payments may be higher because the need to provide such assistance quickly can detract from the planning and implementation of effective controls. Our past work has shown that federal agencies should better

[19]https://gaoinnovations.gov/antifraud_resource/ and GAO, *A Framework for Managing Improper Payments in Emergency Assistance Programs*, GAO-23-105876 (Washington, D.C.: July 13, 2023). Payment integrity includes efforts to minimize all types of improper payments—payments that should not have been made or were made in the incorrect amount—whether from mismanagement, errors, abuse, or fraud. While all payments resulting from fraudulent activity are considered improper, not all improper payments are the result of fraud.

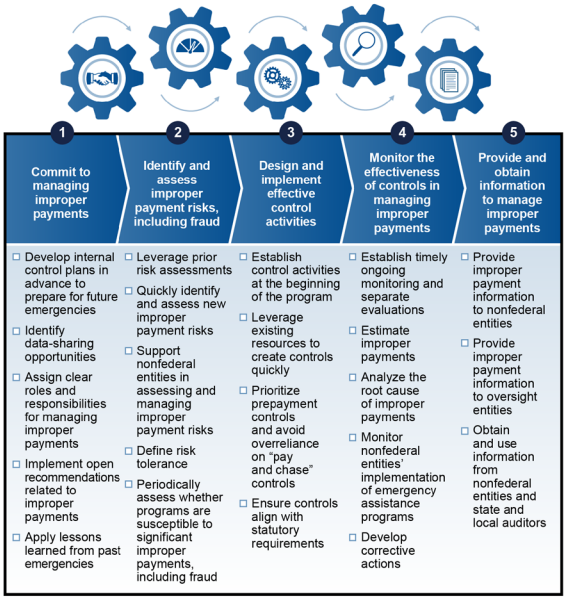
[20]https://gaoinnovations.gov/antifraud_resource/.

plan for and take a more strategic approach to managing improper payments in emergency assistance programs. In response, in July 2023, we published the Managing Improper Payments Framework.[21]

This framework is intended to help federal agencies mitigate improper payments, including those stemming from fraud, in emergency and nonemergency programs before they occur. It can also serve as a resource for Congress when designing new programs or appropriating additional funding in response to emergencies. It identifies five principles and corresponding practices (fig. 6) that align with leading practices from our Fraud Risk Framework, such as identifying and assessing fraud risks that cause improper payments.

[21]GAO-23-105876.

Figure 6: Framework for Managing Improper Payments in Emergency Assistance Programs



Source: GAO (analysis and icons). | GAO-24-107122

In addition, our prior work identified opportunities for Congress to take action to focus agency attention on strategic fraud risk management. These matters for congressional consideration remain open. We continue to believe that such actions will increase accountability and transparency in federal spending in both emergency and nonemergency periods.

Open Matter for Congressional Consideration

Congress should amend the Payment Integrity Information Act of 2019 to reinstate the requirement that agencies report on their antifraud controls and fraud risk management efforts in their annual financial reports.

Source: GAO-24-107122.

Reinstate reporting requirements for fraud risk management. We previously reported that Congress's ability to oversee agencies' efforts to manage fraud risks is hindered by the lack of fraud-related reporting requirements. The Fraud Reduction and Data Analytics Act of 2015 and the Payment Integrity Information Act of 2019 required agencies to report on their antifraud controls and fraud risk management efforts in their annual financial reports. However, the requirement to report such information ended with the fiscal year 2020 annual financial report. Since then, there has been no similar requirement for agencies to report on their efforts to manage fraud risks.[22] In March 2022, we suggested that Congress amend the Payment Integrity Information Act of 2019 to reinstate reporting requirements.[23]

Open Matter for Congressional Consideration

Congress should establish a permanent analytics center of excellence to aid the oversight community in identifying improper payments and fraud.

Source: GAO-24-107122.

Establish a permanent analytics center for identifying fraud and improper payments. Responsibilities for planning and implementing fraud risk management and detection activities start with agency management officials, however, the oversight community plays a critical role in identifying and investigating suspected fraud. The importance of this role in nonemergency periods is heightened during emergencies such as the COVID-19 pandemic as agencies work to implement large-scale relief efforts quickly.

At the outset of the pandemic, there was no permanent, government-wide analytical capability to help inspectors general identify fraud. In March 2021, the American Rescue Plan Act of 2021 appropriated $40 million to the Pandemic Response Accountability Committee, which subsequently established the Pandemic Analytics Center of Excellence (PACE).[24] The role of PACE is to help oversee the trillions of dollars in federal pandemic-related emergency spending. According to the Pandemic Response Accountability Committee, the PACE applies best practices, with the goal of building an "affordable, flexible, and scalable analytics platform" to support Offices of Inspectors General during their pandemic-related work, including beyond the organization's sunset date in 2025.

In March 2022, we recommended that Congress consider establishing a permanent analytics center of excellence to aid the oversight community

[22]The Payment Integrity Information Act of 2019 includes multiple ongoing reporting requirements for agencies related to improper payments generally but none specifically mention fraud.

[23]GAO-22-105715.

[24]Pub. L. No. 117-2, 135 Stat.4.

in identifying improper payments and fraud.[25] Without permanent government-wide analytics capabilities to assist the oversight community, agencies will have limited resources to apply to nonpandemic programs to ensure robust financial stewardship, as well as to better prepare for applying fundamental financial and fraud risk management practices to future emergency funding.

Open Matter for Congressional Consideration

Congress should amend the Social Security Act to accelerate and make permanent the requirement for the Social Security Administration to share its full death data with the Department of the Treasury's Do Not Pay working system.

Source: GAO-24-107122.

Amend the Social Security Act to make permanent the sharing of full death data. Data sharing can allow agencies to enhance their efforts to prevent improper payments to deceased individuals. To enhance identity verification through data sharing, we have previously suggested that Congress consider amending the Social Security Act to explicitly allow the Social Security Administration to share its full death data with Treasury's Do Not Pay system, a data matching service for agencies to use in preventing payments to ineligible individuals.[26] In December 2020, Congress passed, and the President signed into law the Consolidated Appropriations Act, 2021, which requires the Social Security Administration to share, to the extent feasible, its full death data with Treasury's Do Not Pay working system for a 3-year period, effective on the date that is 3 years from enactment of the act.[27] In March 2022, we suggested that Congress accelerate and make permanent the requirement for the Social Security Administration to share its full death data with Treasury's Do Not Pay working system.[28]

Chairman Schweikert, Ranking Member Pascrell, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions.

[25]GAO-22-105715.

[26]GAO, *Improper Payments: Strategy and Additional Actions Needed to Help Ensure Agencies Use the Do Not Pay Working System as Intended*, GAO-17-15 (Washington, D.C.: Oct. 14, 2016) and *COVID-19: Opportunities to Improve Federal Response and Recovery Efforts*, GAO-20-625 (Washington, D.C.: June 25, 2020).

[27]Pub. L. No. 116-260, div. M and N, 134 Stat. 1182 (2020).

[28]GAO-22-105715.

GAO Contact and Staff Acknowledgments

For further information about this testimony, please contact Rebecca Shea, Director, Forensic Audits and Investigative Service, at (202) 512-6722 or shear@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Gabrielle Fagan (Assistant Director), Lauren Kirkpatrick (Analyst-in-Charge), Irina Carnevale, Leia Dickerson, Paulissa Earl, Maria McMullen, Sabrina Streagle, and Nick Weeks.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts. Visit GAO on the web at https://www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact FraudNet: Website: https://www.gao.gov/about/what-gao-does/fraudnet Automated answering system: (800) 424-5454 or (202) 512-7700
Congressional Relations	A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548
Strategic Planning and External Liaison	Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548

Chairman SCHWEIKERT. Thank you, Ms. Shea.
Mr. Asaro-Angelo.

STATEMENT OF ROBERT ASARO-ANGELO, COMMISSIONER, NEW JERSEY DEPARTMENT OF LABOR AND WORKFORCE DEVELOPMENT

Mr. ASARO-ANGELO. Good morning, Chairman Schweikert, Chairman Smith, and Ranking Member Pascrell, members of the Subcommittee on Oversight, and to all your hard-working members of your staff. Thank you for inviting New Jersey to this important conversation. I can assure my colleagues to my right that anti-fraud measures have always been a priority in New Jersey.

In the winter of 2020, we were in great shape, with record numbers of people working. Nobody could have predicted the economic and personal chaos of the global COVID–19 crisis. From February to April, in just 2 months, our state lost over 730,000 jobs, more than 1 in 6. On April 1, we saw a 2,700 percent increase in UI claims from that same week the prior year—2,700 percent.

With Congress's quick action through the Families First Coronavirus Response Act and the CARES Act, we provided lifelines to those who needed help staying afloat when they lost their jobs. In just 21 months, we distributed close to $40 billion to 1.6 million workers. But, unfortunately, there are those who took advantage of the situation as an opportunity for ill-gotten gain.

Since New Jersey has a higher-than-average benefit rate, we have always taken fraud very seriously. We have instituted aggressive measures and applied several anti-fraud processes. We rely on this layered approach, from analytics to third-party identity-proofing, to both catch suspicious claims and act as a deterrent, greatly reducing fraud attempts to begin with.

Prior to the pandemic, UI fraud generally meant someone was illegally collecting benefits while working, or otherwise being dishonest on their application or weekly certification. Identity theft had been a long-time but manageable issue. But now, with the vast amounts of personally identifiable information—or PII—available on the dark web, fraudsters were ready to weaponize it.

To be clear, I am not just talking about domestic attacks. There are global fraud rings, as mentioned earlier, who share vulnerabilities of various state systems and cherry pick the ones easiest to deceive.

With a dramatic increase in claimants and a dramatic increase in benefits, there is a dramatic increase in fraudulent claims. Fraudsters saw the pandemic as the perfect time to attack, as—and they saw almost—an almost perfect target: Pandemic Unemployment Assistance, or PUA. While enacted with the best of intentions, PUA added a whole new population of beneficiaries to our system that we had never had before. We simply did not have the mechanism and, more importantly, the statutory authority to verify their employment.

For PUA, eligibility was based solely on self certification, and states were prohibited by law from confirming this information: the perfect recipe for fraud. Unlike regular UI, where every individual claim is verified or contested by an employer, a crucial backstop for fraud, states didn't have the ability to check this information until

the end of 2020 with passage of the Continued Assistance Act. The constantly changing rules, along with the pressure to get these payments out as quickly as possible, made every state all the more vulnerable.

So the challenge during the height of the pandemic and still to this day has been balancing our efforts to get payments out quickly to the claimants who deserve them while safeguarding our trust fund from cheaters and criminals. And these steps take time.

During the pandemic our anti-fraud efforts were challenged like never before, battling dark web tutorials on how to commit fraud, caches of stolen PII, and tutorials on social media with step-by-step instructions on how to commit fraud to get benefits. But our seasoned professionals rose to the occasion, identified risks, acted swiftly, and went above and beyond their traditional fraud prevention and risk management operations.

Our Cyber Fraud Investigations team was created out of necessity during the pandemic due to the tremendous and relentless attacks. They teamed up with our IT division to combat the cyber-fraud attempts, with a focus on technology to support their efforts. Partnering with ID.me, a federally-credentialed security vendor, New Jersey became the first state to offer three ways to digitally verify claimant identity that all meet heightened Federal security standards: self-service, live video chat, and in-person. During the pandemic, New Jersey halted hundreds of thousands of fraudulent payments, protecting billions of dollars.

Although claims have slowed overall, including false ones, we are always shoring up our defenses. Through the National Association of State Workforce Agencies, or NASWA, we are collaborating with other states to share findings, trends, and best practices. The funding we have received through the American Rescue Plan to modernize our unemployment system has been critical. Building a newer, more modern system improves equity of access and security, which go hand in hand with fighting fraud.

It is vitally important we continue supporting efforts for national improvements to create overarching systems that work with each other, instead of having each state operate independently. Fraudsters love nothing more than having 53 separate systems to pick through to see which can be hit the easiest and the hardest.

There is no silver bullet to completely eradicate fraud from our benefit system, but we can combat it in every way possible, continually learning and training so we stay one step ahead. We look forward to working with our Federal partners across multiple agencies to combat fraud, apply lessons learned, solidify policies, and see concrete action at the national level to ensure we never see such widespread UI fraud ever again.

I am grateful for this time to speak with you all. I am happy to address any questions you may have to the extent that I can without revealing any of our trade secrets to the fraudsters who are most certainly watching this hearing. Thank you.

[The statement of Mr. Asaro-Angelo follows:]

Oversight Subcommittee Hearing on Investigating Pandemic Fraud: Preventing History from Repeating Itself

Thursday, October 19, 2023, 10 a.m. (testimony due Tuesday, Oct. 17)

Good morning Chairman Schweikert, Ranking Member Pascrell, and Members of the Subcommittee on Oversight. Thank you for inviting New Jersey to this important conversation.

In winter of 2020, we were in great shape, with record numbers of people working. Nobody could've predicted the economic and personal chaos of the global COVID-19 crisis.

From February to April – in just two months – our state lost over seven hundred and thirty thousand jobs – more than 1 in 6. In one April week, we saw a **twenty-seven hundred percent (2,700%)** increase in UI claims from that same week the prior year.

With Congress's quick action through the Families First Coronavirus Response Act and the CARES Act, we provided lifelines to those who needed help staying afloat when they lost their jobs. In just 21 months, we distributed close to $40 **Billion** dollars to 1.6 million workers.

But, unfortunately, there are those who took advantage of the situation as an opportunity for ill-gotten gain.

Since New Jersey has a higher-than-average benefit rate, we've always taken fraud very seriously. We've instituted aggressive measures and applied several anti-fraud processes. We rely on this layered approach – from analytics to third-party identity proofing – to both catch suspicious claims **and** act as a deterrent, greatly reducing fraud attempts to begin with.

Prior to the pandemic, UI fraud generally meant someone was illegally collecting benefits while working, or otherwise being dishonest on their application or weekly certification. Identity theft has been a longtime, but manageable, issue. But now, with vast amounts of personally identifiable information, or PII, available on the dark web, fraudsters were ready to weaponize it.

To be clear, I'm not just talking about domestic attacks; there are global fraud rings, who share vulnerabilities of various state systems and cherry-pick the ones easiest to deceive.

With a dramatic increase in claimants – and a dramatic increase in benefits – there's also going to be a dramatic increase in fraudulent claims. Fraudsters saw the pandemic

as the perfect time to attack, and they saw an almost perfect target, Pandemic Unemployment Assistance or PUA.

While enacted with the best of intentions, PUA added a whole new population of beneficiaries to our system that we never had before, and we simply did not have a mechanism – and more importantly, the statutory authority – to verify their employment. For PUA , eligibility was based solely on self-certification, and states were **prohibited** by law from confirming this information – the perfect recipe for fraud. Unlike regular UI where every individual claim is verified or contested by an employer, a crucial backstop fo fraud, states didn't have the ability to check this information until the end of 2020, with passage of the Continued Assistance Act. The constantly changing rules, along with the pressure to get these payments out as

quickly as possible, made every state all the more vulnerable.

So, the challenge – during the height of the pandemic and still to this day – has been balancing our efforts to get payments out quickly to the claimants who deserve them, while safeguarding our trust fund from cheaters and criminals – and these steps take time.

During the pandemic our anti-fraud efforts were challenged like never before, battling dark web tutorials on how to commit fraud, caches of stolen PII, and tutorials on social media with step-by-step instructions on how to commit fraud to get benefits… but our seasoned professionals rose to the occasion, identified risks, acted swiftly, and went above and beyond their traditional Fraud Prevention and Risk Management operations.

Our Cyber Fraud Investigations team was created out of necessity during the pandemic due to tremendous and relentless attacks. They teamed up with our IT division to combat the cyber fraud attempts with a focus on technology to support their efforts.

Partnering with ID.me, a federally credentialed security vendor, New Jersey became the first state to offer three ways to digitally verify claimant identity that all meet heightened federal security standards – self-service, live video chat, and in-person.

During the pandemic, New Jersey halted hundreds of thousands of fraudulent payments, protecting billions of dollars.

Although claims have slowed overall – including false ones – we're always shoring up our defenses.

Through the National Association of State Workforce Agencies, or NASWA, we're collaborating with other states to share findings, trends, and best practices.

The funding we've received through the American Rescue Plan to modernize our unemployment system has been critical. Building a newer, more modern system improves equity of access **and** security – which go hand-in-hand with fighting fraud. It's vitally important we continue supporting efforts for national improvements to create overarching systems that work with each other, instead of having each state operate independently. Fraudsters love nothing more than having 53 separate systems to pick through to see which can be hit easiest and hardest.

There's no "silver bullet" to completely eradicate fraud from our benefits systems, but, we can combat it in every way possible – continually learning and training so we stay one step ahead.

We look forward to continuing to work with our federal partners across multiple agencies to combat fraud, apply lessons learned, solidify policies, and see concrete action at a national level to ensure we never see such widespread UI fraud ever again.

I'm grateful for this time to speak with you all. I'm happy to address any questions you may have to the extent I can, without revealing any of our trade secrets to the fraudsters who may be watching.

Thank you.

###

Chairman SCHWEIKERT. Thank you, Mr. Asaro-Angelo.

All right, as the chairman I guess I get to ask the questions first. Yay.

I still remember when the pandemic started off, and have—how many of you had this family experience where you pick up the phone and it is your wife, and your wife is going, "You know, I am here handling all these unemployment requests" at the surgery center she ran, and a lot of it were people who had never worked there, people who hadn't worked there in years. But the best one was when she was getting unemployment requests or the verifications for herself. And the phone call was, "Do you want me to quit now? Because apparently I am already asking for the unemployment." And okay, a small surgery center, I think they may have had 20 to 30 employees. And she said they added up over that year—hundreds of these came in.

I have a board here, and this is sort of going on the theme—and forgive me, I am going to do something a little awkward, but I don't have a better way to do this. We are trying to not only—and this is going to go to you substantially, Ms. Miller, because you have actually touched on things that everyone else also touched on. We were trying to get our heads around if we had a national data exchange for the verification as our friend from New Jersey just spoke about.

Does it stop it where the identities—the identities are out there, they have been stolen. We have actually, as Members of Congress, had our identities stolen not too long ago. Does it stop it where the actual applying—where in this process—because we have been tracking some crazy stories of UI fraud that was converted to gift cards, that got moved into buying cars, and then the cars were shipped to North Africa as a way to wash the money.

Let's say we had your data exchange. Where do I break the fraud loop, the information, the ability to make the requests?

Ms. MILLER. Yes, well, thank you. The data is the way to address this significant problem, which is identity theft that you are talking about. And we saw unprecedented identity theft because of the vast number of data breaches that we have experienced.

Every single American's information is available for sale on the dark web today. You can buy Social Security numbers for about $0.25 a piece now. They have gone down. There were about $1 a piece about a year ago. And so, as a result of having so much information available for so little money and fraud actors being able to monetize that information, what agencies need at the Federal and the state level is the ability to identify quickly those indicators that would suggest that somebody who is applying for a benefit is, in fact, a stolen identity, things like the device geolocation.

So, in the UI fraud, for example, if somebody was applying for pandemic benefits and they lived in Nigeria, and you were sitting in the UI office in Iowa, you did not have any kind of IP address tracking to know that.

Chairman SCHWEIKERT. But, Ms. Miller, can I bust that by using, you know, a VPN?

Ms. MILLER. Yes. You can—most of these tools to steal—to use—to effectively use stolen identities can be circumvented, especially in the age of generative AI. So now we have even got much

more sophisticated tools than we did at the beginning of the pandemic that they are using and exploiting right now.

And so, as a result, as Amy mentioned, the concept of, you know, a dynamic and a static, we have got a dynamic adversary, and we have very, very static processes that address them. Agencies need to be able to use the kinds of tools that banks use, that technology companies use, that—you know, where they can very quickly identify these patterns. And that is a data problem. And we have a data problem in government.

We are very protective of the privacy of citizen data. And I am not saying we shouldn't be, but in—today, when every single one of our identities are being stolen on the dark web, but the government is protecting our information to the degree that the adversaries can use the data, but the government can't use it to stop them.

Chairman SCHWEIKERT. Okay, and I have a handful of questions, but I want to finish one last with Ms. Miller.

In your testimony, what do I have to change statutorily or redefine statutorily so I don't run into the constant excuse that we often, as Members of Congress—"Well, that has a privacy concern, or that is over there."

Ms. MILLER. Yes.

Chairman SCHWEIKERT. At the same time that these people's privacy has long since been violated.

Ms. MILLER. You know, honestly, I am for privacy. I am a good—I believe in privacy. But the privacy—there is a very, very robust protection of privacy sort of lobby and group on one side, who has gone so far—and it is—we need to consider that we live in a different world now. The Privacy Act and the Computer Matching Act were written at a time that we are in—this environment that we are living in is changing monthly. Literally, it is changing every month. And we have got laws that we haven't changed in years.

So the Privacy Act, the Computer Matching Act, and the Fair Credit Reporting Act, the FCRA, all three of those need to be considered on the basis of how we can better use data to prevent fraud across the government.

Chairman SCHWEIKERT. Okay.

Mr. ASARO-ANGELO. Chairman Schweikert——

Chairman SCHWEIKERT. New Jersey——

Mr. ASARO-ANGELO [continuing]. Back to your original question on that chart—and Mr. Fitzpatrick, I don't want to hurt—with bringing it up again, but, you know, this is where I think we need to marry technology and policy because on that chart you had, you know, the stolen identities, then the applying for unemployment, and then getting the benefits.

Right now, under statute, we have to let everybody apply for UI benefits, no matter if we know that they are stolen in advance. The way this current statute is that we have to let everybody apply——

Chairman SCHWEIKERT. Okay, so——

Mr. ASARO-ANGELO [continuing]. And then do the security check afterward.

Chairman SCHWEIKERT. Say that sentence again. So even when it hits your door, you still have to——

Mr. ASARO-ANGELO. We have to process that application. Now, clearly, the identity verification and all the other checks can be part of that process afterwards. But we can't deny anybody the ability to apply for unemployment benefits at this time.

Chairman SCHWEIKERT. Okay. Ms. Shea—and this is one-off—but I—for my own sanity, I need to ask. Have you seen any research done on how many bad actors around the world this fraud may have helped finance? Because, you know, think about, you know, what is going on in the Middle East right now, and we have had some things come to our office saying some of these organized international criminal cartels were washing the money for violence. Any place I can go to chase that down?

Ms. SHEA. Well, so no specific numbers and amounts, but we did look at some of that information through the Department of Justice press releases on cases. And so, we have some information about foreign actors exploiting the various pandemic programs—in different programs, not just unemployment insurance.

But I do want to get back to this issue of addressing unemployment insurance fraud issues. In 2020, there is an integrity data hub that provides services to states to check the verification of whether or not there is an application across states if somebody applies in multiple states. The bank account verification—it will do a validation of the bank account. It will check to see whether their identity flags on a particular application. In 2020, 34 states participated in that integrity data hub, and the other states did not.

Chairman SCHWEIKERT. For the 34, how effective was it?

Ms. SHEA. Well, notwithstanding some of the issues Rob mentioned about prohibitions against certain checks, it provides information to the states about where there are flags, where there are areas of concern where the payment should not be made. Now, Department of Labor has since been able to get all 50 states and 3 territories signed up for that service. It is a free service. It is available to them.

So I think, as we are thinking about resources and, you know, additional data sources and new technologies that we can be—that can be applied, it is also important to think about what is already available to federally-funded programs and to Federal programs to prevent fraud.

Chairman SCHWEIKERT. Okay, my very last question. Could I take that data hub and enhance it with Ms. Miller's AI and other database touches?

Is there a way that this isn't reinventing the wheel, but making the wheel much more efficient?

Ms. SHEA. I——

Chairman SCHWEIKERT. Now I forced the two of you to talk to each other. [Laughter.]

Ms. SHEA. Yes, that is what really needs to get done. I mean, if we want to fix this, we have to think about the states working together. And so there is this hub that does have—it is—it provides an opportunity for those—for them to share data across the states. If they augment that with third-party data, they are going to have a whole lot more robust data sets to be able to share information and identify fraud schemes much quicker and more effectively.

Chairman SCHWEIKERT. Okay, thank you, witnesses. It is actually appreciated.

Mr. Pascrell.

Mr. PASCRELL. Thank you, Mr. Chairman.

Ms. Miller, we can't legislate directly identity theft. That is my contention. So, we need to work from the front end, and put into legislation reasonable—and unreasonable, sometimes—as you pointed out, we are in a different world—but basically, reasonable attempts to prevent the fraud or the possibilities of fraud from ever happening. That is not only true here, unemployment insurance. We talked about it yesterday, every Federal program.

I am not a—never met anybody on this panel, this committee, on either side—now, no one is privy to virtue in politics. Let's get that straight. But we can't be helpless to the problem, knowing it is going to get worse. The chairman has pointed that out vividly. But everybody on this panel doesn't simply send their support for legislation because so what? Somebody gets it that doesn't deserve it, so what? No, no, that undermines the credibility of the program. You know that better than I do. So, we need to take a very close look at this, and it is a serious, serious problem dealing with serious, serious money.

Mr. Commissioner, the title of this hearing is "Keeping History from Repeating Itself." What are the top things we here can do to keep this criminal activity—this is criminal, what we are talking about here—from happening again? Because there are going to be programs in the future that are ripe for those who wish to deceive. And those who wish to deceive are taking money from their peers who are getting the advantage of the programs.

So I don't want to hear generally about the poor. The poor are many times crooks. Really? Are you serious?

So what do you think we can do about it?

Mr. ASARO-ANGELO. Well, hopefully, we never have to have a situation like COVID ever again. But if one does arise, if some kind of national emergency, don't ever pass a program like PUA again. PUA was primarily for independent contractors and self-employed. It should have been in Treasury or SBA. The 1099 workers, the self-employed are inherently small businesses. PUA was the main cause of UI fraud during COVID, and sort of got the camel's nose under the tent, as they say. In regular UI the employers of the workers are the crucial part of the anti-fraud process.

Congressman Schweikert, you talked about your wife working at the surgery center. That is how we stop fraud. Very often we hear from the employers who say, "Hey, I got a filing for this person, and they don't—one, they don't exist, or two, they don't work for us, or three, they are still employed." That is one of our most important ways to fight fraud.

Mr. PASCRELL. The specifics that you are talking about, would you please, at your leisure, put them down in very specific order in terms of the—being in parallel to what you testified today, and get it to everybody on this panel? I would ask you to do that. Is that asking too much?

Mr. ASARO-ANGELO. Not at all, Congressman.

And to answer Congressman Schweikert's question of before——

Mr. PASCRELL. And let me ask——

Mr. ASARO-ANGELO [continuing]. He does know everybody in New Jersey, yes.

Mr. PASCRELL. Thank you. Every Democratic member on this panel worked very closely with the President to include $2 billion. Correct me if I am wrong, anybody—for unemployment insurance fraud-fighting measures in the landmark the American Rescue Plan was not that long ago.

Can you provide some examples of how New Jersey spent these Federal dollars to modernize its UI program in support of workers to prevent fraud?

Mr. ASARO-ANGELO. There is a lot. I will try to keep it really brief.

We have increased staff, fraud staff specifically, with the creation of our cyber fraud investigations unit. We contracted with an identity credentialing vendor. We have—now we have a dark web monitoring service. We procured IT services to enhance an existing data analytical tool, which allowed us to ingest numerous data elements like Ms. Miller talked about to identify fraud trends and patterns. Supported our pilot, along with Arkansas from U.S. DOL, our claimant experience pilot, which informed much of our current research and best practices on our new application, which we will launch in just a couple of weeks. We established our Office of Unemployment Modernization to deliver a UI system built with smaller modular pieces, not one big chunk all at one time. That usually leads to failure. And all other forms of our UI modernization, which is always going to make our systems more secure.

Mr. PASCRELL. Go ahead.

Chairman SCHWEIKERT. Mr. Pascrell, are you telling me I have things to learn from New Jersey?

Mr. PASCRELL. Yes.

Chairman SCHWEIKERT. We are going to go to two-to-one on this, just because we are running into some interesting conference time.

Mr. Fitzpatrick.

Mr. FITZPATRICK. Thank you, Chairman Schweikert, for holding the hearing. My first question is for Ms. Miller.

In December of 2022, the Secret Service announced that hackers linked to the Chinese Government stole at least 20 million in U.S. COVID relief benefits, including UI funds in over a dozen states. A former assistant U.S. attorney who indicted these hackers from this Chinese criminal group in both 2019 and 2020 said that the hackers have "tens of thousands of machines" going at one time to obtain personally identifiable information and generate criminal profits.

Even more concerning, officials and experts told one media outlet that other Federal investigations of pandemic fraud seem to point back to foreign state-affiliated hackers. So, my question, Ms. Miller, American officials have blamed Chinese hackers for the breaches of OPM, of Anthem Health, and Equifax. And it is clear that COVID fraud is not just a domestic issue; this is a matter of national security.

So, based on your experience working with the Pandemic Response Accountability Committee, which is a member of, of course, of DOJ's International Organized Crime Intelligence and Oper-

ations Center, what are the national security implications, in your view, of foreign state-affiliated hackers stealing taxpayer funds that were intended to be for COVID relief benefit programs?

Ms. MILLER. Yes, we—data on this is still being evaluated. But there are some estimates that half of the Pandemic Unemployment Assistance fraud went to adversarial nations, and that is pretty problematic when you consider that people, when they think about fraud, they think, oh, it is just a little rounding error, it is a problem. These are—this was fraud that is funding our adversaries. That is what happened during the pandemic, and that is why there is so much attention on it, which is valid.

These hackers—and they—there is a full underground market of fraud actors today. We call it fraud as a service. And it is a full—those fraud actors, they have at their disposal really sophisticated artificial intelligence tools. They have the flexibility and agility to be able to move. If something is not working, they can just take something down and put it back up. We have seen where the DOJ has taken down a malware site, and it has been back up two months later, and it is even more effective.

So we cannot fight this adversary the way that we are currently fighting this adversary, because this adversary is serious, and they are looking to steal money to create not just a financial problem, but a national security problem.

Mr. FITZPATRICK. Thank you, Ms. Miller.

Ms. Shea, what are the existing tools that agencies can be using to prevent money that is fraudulently claimed from going out the door?

Ms. SHEA. So GAO is dedicated to helping agencies enhance their strategic approach to fraud risk. You know, we are always going to come back to what it is that the program managers can do. And, you know, you are hearing a lot about the risk involved.

And so trying to encourage them to better understand that risk so that they can strategically plan for it, identify what the best solutions are. And we do that through things like our fraud risk framework, which lays out 38 leading practices, a roadmap for agencies to understand how best to strategically manage risk. We have developed an anti-fraud resource, which is a web-based, interactive, user-friendly guide that lays out the who, what, when, where, why, and how of, you know, how fraud happens, so that they can understand and take action.

There are other tools and resources like Treasury's Anti-Fraud Playbook, which helps agencies figure out how to best manage their risk and understand them, so—in addition to a couple of matters that we have recommended to Congress to take to help address these issues.

Mr. FITZPATRICK. And in your position of director of forensic audits, you made recommendations to Federal agencies on how to improve their fraud prevention.

So, number one, have the agencies agreed with those recommendations?

And number two, have they implemented those recommendations?

Ms. SHEA. So we have made a number of recommendations in, you know, normal operations and, of course, in the COVID pro-

grams. And I would say about 27 overall, 28 overall related to COVID-specific fraud risk management, and there are still, I think, about 18 of those left open.

So agencies do not always agree, and that is true in normal operations. We don't always get agreement. And that relates back to the mindset issue. They aren't always appreciating the risk that exists.

Mr. FITZPATRICK. Thank you. Thanks to the panel for being here.

I yield back.

Chairman SCHWEIKERT. Thank you, Mr. Fitzpatrick.

Mr. Steube.

Mr. STEUBE. Thank you, Mr. Chairman.

The COVID–19 pandemic and the resulting shutdowns imposed tremendous costs on our nation. Unfortunately, criminals exploited our dysfunctional Federal Government to steal American taxpayer funds intended to alleviate the suffering. This resulted in the fraudulent transfer of over $280 billion to criminals, according to an Associated Press analysis. American taxpayers were fleeced, and their government failed in its duty to protect their tax dollars.

GAO has estimated the unemployment fraud during the pandemic may reach as high as 135 billion. That figure represents 15 percent of all unemployment insurance benefits paid out during the pandemic. Meanwhile, criminals further victimize American citizens through identity theft schemes. The Federal Trade Commission reported a 3,000 percent increase in identity theft claims related to government benefits in 2020. This caused difficulty in accessing benefits for many law-abiding Americans.

The sad fact is that much of this could have been prevented. The Federal Government should be better stewards of the hard-earned dollars American families pay in taxes. Law enforcement must track down these criminals and recover the illegally-obtained funds, but we also need to plan for the future to ensure this never happens again. The tools exist for the Federal Government to prevent this kind of fraud, we just need to make sure that the tools are actually used.

Ms. Miller, the Pandemic Response Accountability Committee, where you served as the deputy executive director, developed an analytics tool called the Pandemic Analytics Center of Excellence, which used analytic technology to uncover patterns, anomalies, and red flags that point to potential fraud. This tool has been used by numerous law enforcement agencies to open over 500 investigations into 6,000 subjects, representing an estimated potential fraud loss of 500 million.

Can you comment on the development of the PACE tool, as well as other ways that technology can be used to address fraud in the future?

Ms. MILLER. Yes, thank you. The PACE is one of the bright spots in government anti-fraud activities that is in the history of American government. The PACE has created a center of excellence, a center, a hub. They—and they negotiated 95 data use agreements. Honestly, that is probably the biggest accomplishment of the PACE.

It is—I can't overstate how challenging it is for agencies to share data. They actually usually just stop trying because of how hard it is to put a data use agreement in place. But because the PACE's whole focus was on trying to gather a lot of data in one place in order to use it to prevent fraud, they were able to get those 95 data use agreements in place. They also have FinCEN data, they have suspicious activity reports data. They are using a lot of third-party data, and they are using really impressive artificial intelligence tools. This should be the model going forward.

And—but my—the important point I want to make, though, is that is only for investigations. We know that we recover about $0.50 on every dollar of fraud that has been stolen. And with identity theft it is even less than that. We need a PACE inside of the management side of government, so that these kinds of tools can be used prior to making a payment, which is why I have been advocating for the creation of a management-side center of excellence. Where that sits is open to discussion. Treasury could be one area that you could put it in, but it needs to have the same capabilities, and it needs to have that dedicated focus because, again, the people at the PACE, that is their entire job is negotiating data sharing agreements, acquiring data, pulling data scientists in.

The other thing the PACE did was create a data science fellowship, and they were able to get recently-graduated data scientists from different universities to come and work on these projects. It is very difficult to get the data science resources within the Federal Government. And so such an analytic center of excellence sitting on the management side should also look at that as a model in order to acquire the data science expertise that is needed.

Mr. STEUBE. So you are proposing the creation of a dedicated anti-fraud office for basically the entire Federal Government. What is preventing agencies from using these existing tools to protect against fraud instead of creating that?

Ms. MILLER. So agencies, number one, most of them don't have—they will tell you—I am not there, but they will tell you that they don't have the resources. They will say, hey, our—and this is—this gets back to this whole incentives piece. They will say, "Our job is to get a benefit out. That is our job. Our mission is benefit delivery. Our mission is not prevention of fraud. That is the IG's mission." And the focus, what we have been trying to do at GAO, and when I was at GAO and ever since, is trying to get agencies to understand that their job is to prevent fraud.

But until they don't—so they will say they don't have the resources, they will say that they don't have the ability to get the data. They will tell you that the data is the problem. The problem is partly because they can't negotiate these data sharing agreements, it is partly because they think privacy laws and FCRA requirements limit them from using that data. So they will tell you all kinds of things. But really, the challenge is that they are not sitting in this hearing today. And, you know, typically we weren't having hearings about fraud until the pandemic happened. Once they sit in the hot seat, I think you will start to see them take this more seriously.

Mr. STEUBE. All right, thank you. I have seven seconds.

So, Ms. Simon, are—can you just explain quickly some cases which COVID relief benefits were stolen and subsequently used for criminal activity?

Ms. SIMON. Certainly. Just one quick P.S. on Linda's point. When I was in the Department of Labor and we tried to get data on incarcerated individuals at the Federal level during the pandemic, which, as you know, would have been very helpful, we ran straight into a brick wall of legal and financial obstacles. And so I just want to say, from experience, that is an incredibly real reality.

Yes, pandemic fraud is effectively a vertical for many criminal organizations, and it is an income source. And there was a recent DOJ indictment, I believe, in Michigan that was a sprawling scheme that was funded by multiple kinds of pandemic fraud, including unemployment, that had murder for hire as one of its services. So these are not run-of-the-mill, someone down the street claimed a few extra weeks that they shouldn't have claimed. This is serious street crime.

Mr. STEUBE. Thank you for being here today.

I yield back.

Chairman SCHWEIKERT. Thank you, Mr. Steube.

Ms. Chu.

Ms. CHU. Yes, I would like to start by reminding my colleagues that the Pandemic Unemployment Assistance program was authorized by the CARES Act and extended by the Consolidated Appropriations Act of 2021, both in overwhelmingly bipartisan votes.

Additionally, Ways and Means Democrats secured funding to fight fraud and recover taxpayer dollars in the American Rescue Plan.

The pandemic was an unprecedented disruption of our economy, and we hope that this does not happen again. But what was clear was that there was necessity for benefits, unemployment benefits, and that is why Democrats and Republicans acted together to expand unemployment benefits as quickly as possible to assist American families who, through no fault of their own, suddenly found themselves without a way to provide for their family's basic needs. This was a success, which is why the U.S. has had a stronger economic recovery than any of our peers.

From my district, I have heard from many individuals that federal pandemic unemployment benefits were a lifeline for providing for basic necessities like food and lifesaving medications. That includes Gretchen from Altadena, California, who has been in the film and television industry for the last 30 years, and is a cancer survivor whose medical coverage is predicated on the number of hours worked; and Mary from Pasadena, California, a nursery school teacher whose employer's doors closed and had to file for unemployment for the first time in her 26-year career; and May, the primary breadwinner for her family living in Sierra Madre, trying to stay afloat, all while distance learning with her three kids. The swift action of Congress mitigated the hardship that jobless workers and their families suffered, and it was essential in stabilizing an economy that lost a staggering 22 million jobs in just 2 months in early 2020.

We know that there are lessons to be learned from these efforts that can strengthen and sustain the UI system for future emergencies, and I hope that it is the goal of the hearing to not neglect our duties to protect our workers in the midst of a global pandemic.

So, Mr. Asaro-Angelo, I do want to note that Democrats took the issue of fraud seriously as part of the American Rescue Plan Act, or ARPA. Democrats provided the Department of Labor with $2 billion to strengthen the integrity and preparedness of state UI systems, as well as to provide grants to states for fraud detection and prevention and overpayment recovery efforts. However, earlier this year, the Fiscal Responsibility Act of 2023 rescinded ARPA funding for UI programs and reduced the total funding for UI programs from 2 billion to $1 billion.

So, in your testimony, you mentioned that New Jersey used these funds to modernize your unemployment system. Can you talk about how these modernization efforts are critical to preventing fraud, and what would be the impact on fraud mitigation by cutting these funds?

Mr. ASARO-ANGELO. Thank you for your question, Congresswoman.

Yes, as I mentioned earlier, these funds have been critical because modernization is key to fighting fraud as well. And the important part of this is that modernization doesn't end, and I think it has been a real problem for our systems for far too long that a state would spend millions of dollars—sometimes hundreds of millions of dollars—to go get a procurement for a new system that may or may not have included anti-fraud measures. Then years later, they would be delivered this system that is already out of date, and any changes they want to make to that system they need to go back and get change orders, get a new contract. I don't think I need to tell anybody here government procurement is not fast or agile.

But what we have done is used the agile method using the GSA contract, where we are working with a team, a vendor team that is working together about building this product, about building small modular parts, which was considered in ARPA, by the way. That way, not only can we be more agile about putting new programs in, we can share them with other states.

And the funding that came out of the ARP for modernization specifically states that states who use these funds have to be able to share that with other states, because right now, when you go to the vendor, they own the code, for the most part, and sharing amongst states on this stuff is very difficult. So I am really thrilled that the U.S. DOL put that in their grant writing for the modernization. We were very proud to receive one of the $11.35 million grants. Because of that rescission, though, not every state could receive it. It became a competitive process, as opposed to every state receiving those dollars. So—but it was very smart how they wrote that—whenever dollars are being used out of that, we have to be able to share that product and those victories with other states, as well.

Ms. CHU. Very good.

I yield back.

Chairman SCHWEIKERT. Thank you, Ms. Chu.

Ms. Tenney.

Ms. TENNEY. Thank you, Mr. Chairman and Ranking Member, and thank you to the witnesses. Great testimony, lots of great documents in here. I really appreciate it.

And I come from New York State, which got a tremendous amount of money for unemployment insurance and a tremendous amount of fraud. And I just wanted to address this first, I think, to either—well, first I will go to Ms. Miller. Maybe Ms. Simon first, and then, Ms. Miller, have you comment.

The previous Department of Labor OIG report provided oversight on the Unemployment Insurance Program stated that some internal controls had traditionally been used or recommended by—to the states but were not used. So, I cite back to a recent committee hearing that we had with the Office of the Inspector General wherein they cited the State of New York was warned back in 2010 that they did not have adequate controls in place to handle the existing unemployment insurance claims that they had.

And I will just give you a—pre-pandemic, an improper payment amount was roughly about 10.34 percent. After the pandemic it was almost 30 percent. The fraud rate of 4.5 percent—and this is before pandemic, with poor controls in place—it went to almost 18 percent. The claims before the pandemic in 2019, the quarter before, there were $530 million in claims went to—in 2021, after the first quarter of 2021, went to 6.5 billion, from 530 million to 6.5 billion, an 1,124 percent increase in claims because of the lack of New York State to have controls.

And while my colleague wants to make this partisan, all of this information is coming from Democratic Comptroller Tom DiNapoli, who has provided numerous reports on warning New York on what is happening to taxpayer money.

And the reason I am so concerned about this is we have created this huge burden on our unemployment insurance trust fund and that our small employers, who were forced to lay off during the pandemic, are now paying for this, as are New York State taxpayers, because the funds were squandered that came through either the American Rescue Plan or other CARES Act monies.

What can we do to get New York up to speed, and really being a true, sound steward of taxpayer dollars that have been wasted?

And, you know, you mentioned, you know, ring—international rings up to 50 percent of the monies. What can we do? What can New York do today to protect its small businesses and its taxpayers in preventing this colossal fraud that we have seen, largely due to the inability of the Department of Labor in New York State to properly implement programs?

What can we do, like today, in the next few months, to curb the costs that we are seeing to prevent this fraud?

And, Ms. Simon, I think I will address it to you first, and then maybe Ms. Miller.

Ms. SIMON. Certainly. I think the one thing that—specifically about this hearing and the question that you asked is that the questions I have started asking when I look at a state's posture is, are the use cases across the fraud life cycle being addressed? So——

Ms. TENNEY. Is your microphone on?

Ms. SIMON. I think so. Should I——

Ms. TENNEY. Yes, talk right——

Ms. SIMON. Can you hear me? Okay.

Chairman SCHWEIKERT. You have to be really close.

Ms. SIMON. Okay, perfect. One of the questions I ask is, if you think about the use cases across the fraud life cycle and ask hard, specific, clear questions of the New York Department of Labor before a claimant applies, "What tools do you have, what information are you getting, what are you doing with that information as the claimant is applying, how are you verifying their identity, what do you do with high-risk identities," and then, after they have applied, "When you see suspicious activity, how do you handle that? What tools do you have in place? What processes, how many fraud investigators do you have? How many cases are going to prosecution?"

But those kinds of questions have not traditionally been asked to state departments of labor, certainly not by Federal counterparts. And often folks like the state auditor are the ones asking those questions.

So I am happy to have a conversation also offline, and give you specific advice. But I think one of the questions is to get very, very specific about the entire life cycle. What is the state doing? What tools does it have in place? And what is it doing with the information it gathers?

Ms. TENNEY. Thank you.

Ms. Miller, if you could just———

Ms. MILLER. Yes, I would just———

Ms. TENNEY. Just a plan.

Ms. MILLER. Sure. I mean, I just think———

Ms. TENNEY. To start.

Ms. MILLER [continuing]. One of the things is, though, is when no one else is looking.

So who calls one of you guys? Someone who says they didn't get a benefit, right? Nobody really calls and says, "Oh my God, there is a ton of fraud in the UI program." That only happens later, when the IG puts out a report and everyone gets alarmed. And so when this is done, and when this blows over, they are still going to go back to worrying about getting that benefit out quickly, because that is who they are going to hear from. They are going to hear from a congressperson when a constituent is saying, "I am not getting my benefit."

So I am going back to incentives to fraud prevention. Internal controls is not exciting stuff. They don't want to worry about internal controls until there is a hearing. And so we have to—you, Congress, has to incentivize them and build this into their performance metrics: "We are glad you are getting benefits out the door quickly, but we also want to make sure that you are doing things to make sure only eligible benefits—beneficiaries are getting those benefits, and not just worrying about the squeaky wheel, which is did I get my benefit and did I get it quickly?"

Ms. TENNEY. Right, yes. We keep flooding these agencies with billions of dollars in taxpayer money, and we are hurting our small business community.

So, thank you so much for your expertise, I appreciate it.

Chairman SCHWEIKERT. Thank you, Ms. Tenney.

Ms. TENNEY. I yield back.

Chairman SCHWEIKERT. Those are terrific questions.

Mr. Feenstra.

Mr. FEENSTRA. Thank you, Chairman Schweikert and Ranking Member. Thank you very much.

I want to also thank our witnesses, and for all your information that you have given. To me, it is all about solutions. We have got to figure out solutions. We have got to really dig down and understand. Obviously, we know what is happening and we have improper payments, we have fraud, we have waste. We have criminals trying to take advantage of our taxpayers. So here is my question to Ms. Miller and Ms. Simon.

We have AI. We have private companies that deal with this all the time. When it comes to credit card companies, they do a great job. We have bank companies that are also doing the same thing. What can we take from them, as a Federal Government and say, hey, let's apply this to what we are doing and to reduce this fraud?

And Ms. Miller, first, how can we handle this? I mean, how can we identify the fraud with these new techniques, and then how can we apply it?

Ms. MILLER. Sure, yes. We—the private sector has really, really advanced tools that they use at the front of what they call the front of the sale, so at the very beginning, right? So when someone is applying for a new benefit, if they are opening an account at a bank, or if they are looking to make a transaction, the bank can very quickly, in what they call in their words as a low-friction technology, right?

They can take a ton of data about me when I apply and say this looks like Linda's—we have seen this Social Security number and this address associated with Linda, but we have never seen it coming from that IP address. Or, you know, this person says that they are applying for this benefit here, but we have information that shows that that bank account is actually in an entirely different state, or maybe even a different country.

Mr. FEENSTRA. Right.

Ms. MILLER. And so they are able to take all that kind of information and triangulate it.

They are also able to say, oh, this new applicant for this loan is actually affiliated with four other people, all of whom have been indicted with—for fraud. This looks like this person might be a shell company associated with a number of—in a fraud ring.

These are the things that the private sector can do. The government has very little, if any, ability to use that kind of data to make those determinations. And that is why the———

Mr. FEENSTRA. Why not?

Ms. MILLER [continuing]. Fraud actors are———

Mr. FEENSTRA. Well, why can't we use that data?

Ms. MILLER. Well, partly it is that most agencies don't even—honestly, most of them don't even know that these are capabilities they can have. There needs to be a lot more education of agency leadership, of what kinds of tools could they put in place.

But again, it gets back to no one is really telling them this is an important priority. So when they get a budget, their budget is focused on getting benefits out the door, it is not focused on preventing fraud. If instead there is built in this money here, we are

going to give you this $10 million, but we expect you to use 1 million of that to build in fraud prevention tools using data———

Mr. FEENSTRA. Yes.

Ms. MILLER. And if they are told that, then they can go and find those. But right now they are not even looking for it.

And so you see things like the Inflation Reduction Act or the Infrastructure Act, where money is going out to states and local governments all across the country. There is very likely enormous fraud in those programs, and there is very little fraud prevention tools being used today.

Mr. Feenstra. So it is the dollars and it is the technology. And that is why I am saying———

Ms. MILLER. Exactly.

Mr. FEENSTRA [continuing]. This is ripe for AI.

Ms. MILLER. Yes.

Mr. FEENSTRA. I mean, absolutely, we—I mean, we have to look at the private sector and solve our problems with what they have been experts on.

Ms. MILLER. Yes, and you can use large language models like———

Mr. FEENSTRA. Yes.

Ms. MILLER [continuing]. Generative AI, like a ChatGPT to—within seconds you could take applications to a program and identify anomalies.

Mr. FEENSTRA. I understand.

Ms. MILLER. You could identify text that is duplicative that indicates that someone is using the same information.

Mr. FEENSTRA. Agreed.

Ms. MILLER. This could be done in seconds if agencies could adopt those technologies.

Mr. FEENSTRA. Thank you.

Ms. Simon, if you could, add on to this. I mean, and what are your thoughts on—I mean, I just don't see this as rocket science. It is just a matter of getting the tools to our Federal Government.

Ms. SIMON. Absolutely. So I think two things.

One, to underscore both of your points, I had a vendor call me. This was after I left government. This is a vendor that is used by most of the large banks for that front-end piece sort of intelligence. And he said, "I have been calling state workforce agencies and I can't get people to call me back. I want to help. I want to be part of the solution."

So, I think, on one side, there is—that is an issue. However, it would be unfair to say workforce agencies if we didn't acknowledge the administrative funding struggles that they have. There is not a dedicated line of funding for fraud. I think there should be, quite frankly. The———

Mr. FEENSTRA. So the cost—it is really the———

Ms. SIMON. But———

Mr. FEENSTRA. I mean there are not dollars to do this. Is that a fair statement?

Ms. SIMON. That—the dollars are not prioritized to do that, so the trade-offs are extremely steep for states.

Mr. FEENSTRA. Got you.

Ms. SIMON. And so I think thinking about the funding that, if we want fraud to be part of the mission, then the funding—the mission funding needs to involve fraud-specific funding.

Mr. FEENSTRA. Right. And I would like to see the ROI on this.

Ms. SIMON. Yes.

Mr. FEENSTRA. I mean, return on investment of saying, all right, if we put X amount of dollars for prevention, what do we get back in return? And not only that, you are protecting your taxpayers. So I just think this is not hard to solve, but we just, as a government, got to do it.

With that I yield back. Thank you.

Chairman SCHWEIKERT. Thank you, Mr. Feenstra.

Mr. Pascrell would like to touch base on something you were speaking of.

Mr. PASCRELL. I have no problem with what you just produced, I really don't. However, if you turn to what I think is a parallel example: the IRS, in terms of the debates we had over that. Again, neither side is privy to virtue.

But the point is, some folks use the data that you talk about to destroy the program. And I am very fearful of that. You may say, well, you are too fearful, but that is my thought in my mind.

Mr. FEENSTRA. And there has got to be protections for that, 100 percent.

Mr. PASCRELL. Well, I hope they stand up.

Mr. FEENSTRA. Yes, that is right.

Chairman SCHWEIKERT. Okay. For both of you, let's have a side conversation, because I think there is a simple technology solution that actually fixes for both of your concerns.

Ms. Moore.

Mr. PASCRELL. Thank you.

Ms. MOORE. Well, thank you so much, Mr. Chairman, for convening this hearing, and I do want to thank our panel for their patience and their extraordinary testimony, extraordinary efforts to stop fraud and abuse.

I do want the chairman to know that I had my very first vanilla cappuccino. [Laughter.]

Ms. MOORE. I am not going to become a latte liberal. [Laughter.]

Ms. MOORE. I am from the Midwest. We just drink plain old coffee all the time. But I do appreciate your effort.

Having said that, I just want to join everyone on this panel to say we are against fraud and abuse. We are against taxpayers footing the bill.

And just to look through some of this extraordinary testimony, I am just looking, for example, with Ms. Simon, with your testimony, I mean, who knew identity theft, synthetic identity, account takeover, phishing schemes, benefit cards, skimming, bribery schemes, self-dealing, document fraud, bot attacks—I mean, not to mention places like Wisconsin, where our technology for unemployment—and I think you made this point, Mr. Asaro-Angelo, was from 1970. I don't even think you have to be all that bright to figure out how to breach something like that.

That being said, you know, at the beginning of the pandemic, 22 million people lost their jobs due to no fault of their own. And just

looking at the material here, it seems like we had a surge of like 33 million extra unemployment claims.

And one of the things that I guess I want to hear from the panel is we had a hearing earlier on this committee—on the full committee—on unemployment fraud, and it seemed that there was a tremendous effort going to be put into going after fraud for people who may not even know that they got an overpayment. I mean, it might have been somebody who got an overpayment of $1,200 they didn't deserve, but we had expanded unemployment benefits. They may not have even known.

And so, I just want to hear from you, maybe Ms. Miller, Ms. Simon, maybe Mr. Asaro-Angelo—I am running out of time—what were the benefits versus the losses that we had in rescuing people from poverty, making sure that some people could pay their mortgages, keep up with their bills, continue consumer spending?

And what message does it send for us to expend government resources running after, you know, Joanne Smith, who got $1,500 she didn't deserve and may not have even known that she didn't deserve it?

Ms. Miller.

Ms. MILLER. Yes, I mean, I think what you are raising is a really, really good point about risk. And when we talk about fraud—and certainly GAO is the expert in this area—focusing on risk is really important. We are not going to get back all the dollars, and they are not all equal. When we are talking about organized crime rims and nation state actors, that is who we need to be focusing on, not someone who got an extra $1,500.

And it is really important, because we don't have the resources anyways, right, to go back and try to go after that money. And we don't want to send that message that it is—you know, we are turning the United States into some sort of police state, where we are trying to make sure that everybody only gets exactly what they are entitled to. That is why we want to use risk, and that is why we want to use data and technology so that we can focus those efforts on those most serious, most egregious actors that are operating rings, and we can do that using technology.

And then, you know, when we have additional resources, the priorities need to be set by the agencies, but the priorities should not be on the small-dollar frauds. The priority should be on the large nation state and organized crime rings. And that is where, I think, all of us up here are in agreement that that should be the focus.

Ms. MOORE. Mr. Asaro-Angelo.

Mr. ASARO-ANGELO. Thank you for your question.

First of all, as far as the overpayments, I am proud that NASWA, which I mentioned before, which includes my counterparts across the country, voted in a unanimous and bipartisan manner to urge Congress to waive all non-fraudulent pandemic-related unemployment compensation overpayments. The amount of time and staff needed to pursue these non-fraud overpayments with a very low return absolutely undermines our efforts at fighting current and future fraud.

Just real quick, I also want to mention we keep talking about as if there is one unemployment system. There are 53 different systems. I mean, if we want to solve or have a way better handle on

the fraud, combine such—have more tools from the Department of Labor, where all states can be talking to each other, where there is one set of applications, one set of security procedures, one set of anti-fraud measures. By these fraudsters being able to pick and choose, they couldn't be happier.

And to—whatever we can do to be talking more—and we do a lot of this through NASWA, and I am very proud of our work on these efforts. The IDH was mentioned before. I must say, though, even though there were only 36 in 2020, it wasn't as important then because it was only regular UI. So we always had the employers as the backstop. PUA made the IDH really important.

So I think if whatever we do can consolidate our efforts across the states and in the Federal Government, that we should be able to do.

Ms. MOORE. Thank you. My time has expired.

Thank you for your indulgence, Mr. Chairman.

Chairman SCHWEIKERT. Thank you.

Ms. MOORE. I yield back.

Chairman SCHWEIKERT. Mr. Davis.

Mr. DAVIS. Well, thank you, Mr. Chairman and Ranking Member, for giving me the opportunity to waive on to this hearing.

Although I am not a member of the subcommittee, my state of Illinois, which is a rather large state, as a matter of fact, had tremendous challenges and problems. But I also remember the great work that the state employment agency did in terms of fielding questions, all the requests that came through.

And so, when we discovered that this kind of fraud was taking place, we were outraged, quite frankly, that criminal rings stole unemployment insurance benefits during the pandemic, which is the reason that we Democrats worked so hard to make sure that we would provide the resources to do something about it. And I can't help but recall that not a single Republican voted for these anti-fraud funds. So we also are proud of the work that we and all of you in the states did to keep workers afloat during the pandemic, which led to the fastest economic recovery in our history.

Commissioner Asaro-Angelo, would forgiving overpayments and you have partially answered that a moment ago, but would forgiving overpayments made to workers who were completely without fault free up resources that your state would need to improve benefit access and prevent future fraud?

Mr. ASARO-ANGELO. There is no doubt about it. The going after overpayments, as I mentioned before, is a really low return on investment. And we also need to remember that during the time of the COVID—the Pandemic Unemployment Assistance, all those programs, the rules were changing, literally, day by day for us and for claimants.

So to have a claimant be in a position where, if you apply in March the rules are different than when you apply in December, or the guidance we are getting from the U.S. DOL, through no fault of their own—very clear, you know, things are changing very quickly—our rules were different almost from week to week. So being able to be eligible one week and not eligible the next week, it was very difficult for our claimants and for our staff, who are newly trained up, newly implementing programs.

So certainly, as I mentioned before, we are all in favor of waiving all non-fraudulent overpayments that came from the pandemic programs.

Mr. DAVIS. And what happened when the pandemic hit to the number of requests for benefits in New Jersey?

Mr. ASARO-ANGELO. Well, during the week of March—ending March 6, we had 7,900 claims; 2 weeks later, during—March 21, we had 155,000 people applied for UI. New claims increased to 205,000 the following week. Within five weeks, we had one million claims in new Jersey.

Mr. DAVIS. Well, I know that you and your staff worked hard to get the benefits out as quickly as you could. What effect did this have on the workers?

Mr. ASARO-ANGELO. Well, I would say the benefits served their purpose, as laid out in statute and regulation and—desire to provide workers with an income during loss of employment and, most importantly, keep them on their feet so that they can look for work while still supporting themselves, their families, and their communities.

The system also helped sustain our economies by sustaining the purchasing power of millions of workers, as Congressman Pascrell mentioned earlier. And so, over the past few years, even with COVID, we have had a remarkable increase in the number of small businesses in New Jersey, and I think largely because of the investment that came through to help workers during this trying time.

Mr. DAVIS. Thank you very much.

And Mr. Chairman, after your treatment of giving me the opportunity to waive on, and also the refreshments that you served, maybe I will waive on——

Chairman SCHWEIKERT. I have a coffee problem, Mr. Davis. I hope everyone else will. But thank you for joining us. And forgive the tyranny of our schedule and our clock.

Mr. Pascrell and I have a running agreement here as part of the discussion that, in many ways, this is shorter than we would like it to be, but one of the more interesting hearings we have ever had. You did something unique as a group, all of you. You actually gave us a path where we think we can do something positive, and maybe make the future more robust, everything from things we are going to need to know how to—New Jersey—meet the privacy standards and the security standards of the Federal Government to the ability—could we actually take what Ms. Miller spoke about, the AI, and Ms. Simon touched on, the—what is available out there, and how it changes so rapidly, and could we ever wrap that around some of the services that Ms. Shea spoke about that already exist?

It is traditional, as the chairman, at the end I need to tell you that you are subject to potential written requests from members that will be made part of the permanent record.

Please be prepared also for maybe more than just two weeks of asking for your help as staff speaks to staff of what could we do to never go through this again.

And with that, this hearing is over.

[Whereupon, at 11:31 a.m., the subcommittee was adjourned.]

MEMBER QUESTIONS FOR THE RECORD

November 6, 2023

Chairman Schweikert,

Thank you for the opportunity to provide a response to a Question for the Record (QFR) following the Oversight Subcommittee Hearing on Investigating Pandemic Fraud on October 19, 2023. You asked me to elaborate and provide sources related to my comment that while data are still being evaluated, there are some estimates that half of pandemic unemployment assistance fraud went to adversarial nations. I would note that this issue is not limited to unemployment assistance but other pandemic programs as well, including the small business loan programs.

There have been numerous references in news articles that allude to estimates of large amounts of pandemic funds stolen by foreign criminal syndicates, rings and/or nation-state actors. I have provided links to the sources and relevant excerpts below. As you can see, there are many different sources and all seem to be speculative at this point, which is why the caveat that data are still being evaluated is so important. Nonetheless, several different sources cite the activity of transnational and or nation state actors from adversarial nations, including China, Iran, Russia and North Korea.

Source #1: Forbes Magazine, December 22, 2021: After A Brazen $400 Billion Unemployment Funds Heist, The U.S. Secret Service Seized Back the Money From Criminals (forbes.com)

> **Relevant excerpt:** *During the chaotic days of the pandemic, it's alleged that an international ring of nefarious fraudsters stole over $400 billion from the U.S. government. This staggering amount is around 50% of unemployment monies paid out.*
>
> *The story sounds like a script for an upcoming movie, starring George Clooney, in which an international collective of bad actors from around the world, including China, Russia, Nigeria, Romania and right here at home, wantonly looted unemployment funds earmarked for out-of-work Americans by perpetrating fraudulent claims. Unknowingly, naive Department of Labor workers sent out checks to bad guys.*
>
> *Axios reported, "Unemployment fraud during the pandemic could easily reach $400 billion, according to some estimates, and the bulk of the money likely ended in the hands of foreign crime syndicates—making this not just theft, but a matter of national security."*
>
> *Blake Hall, CEO, and founder of ID.ME, said, "Fraud is being perpetrated by domestic and foreign actors." He added, "We are successfully disrupting attempted fraud from*

international organized crime rings, including Russia, China, Nigeria and Ghana, as well as U.S. street gangs."

Source #2: NBC News, December 5, 2022: Hackers linked to Chinese government stole millions in Covid benefits, Secret Service says

Relevant excerpt: *The theft of state unemployment funds is the first pandemic fraud tied to foreign, state-sponsored cybercriminals that the U.S. government has acknowledged publicly.*

Hackers linked to the Chinese government stole at least $20 million in U.S. Covid relief benefits, including Small Business Administration loans and unemployment insurance funds in over a dozen states, according to the Secret Service.

The theft of taxpayer funds by the Chengdu-based hacking group known as APT41 is the first instance of pandemic fraud tied to foreign, state-sponsored cybercriminals that the U.S. government has acknowledged publicly, but may just be the tip of the iceberg, according to U.S. law enforcement officials and cybersecurity experts.

The officials and experts, most speaking on the condition of anonymity because of the sensitivity of the subject matter, say other federal investigations of pandemic fraud also seem to point back to foreign state-affiliated hackers.

"It would be crazy to think this group didn't target all 50 states," said Roy Dotson, national pandemic fraud recovery coordinator for the Secret Service, who also acts as a liaison to other federal agencies probing Covid fraud.

The Secret Service declined to confirm the scope of other investigations, saying there are more than 1,000 ongoing investigations involving transnational and domestic criminal actors defrauding public benefits programs, and APT41 is "a notable player."

And whether the Chinese government directed APT41 to loot U.S. taxpayer funds or simply looked the other way, multiple current and former U.S. officials say, the theft itself is a troubling development that raises the stakes. One senior Justice Department official called it "dangerous" and said it had serious national security implications.

Source #3: Testimony of the American Hospital Association for the Subcommittee on Federal Spending Oversight and Emergency Management of the Committee on Homeland Security and Governmental Affairs of the U.S. Senate Cyber Threats Amid Pandemic, December 2, 2020: Link: https://www.aha.org/testimony/2020-12-03-aha-testimony-senate-hearing-cyber-threats-amid-pandemic

Relevant excerpt: *Sept. 16, 2020 the Department of Justice (DOJ) stated in regard to the indictment of two Iranian hackers, "Unfortunately, our cases demonstrate that at*

least four nations — Iran, China, Russia and North Korea — will allow criminal hackers to victimize individuals and companies from around the world, as long as these hackers will also work for that country's government…"5 In another example from Sept. 16, DOJ stated that, "the Chinese government tolerated the defendants' criminal activity because those defendants were willing to work on behalf of the Chinese intelligence services."6

Source #4: CNBC, August 22, 2022: Secret Service returns fraudulent pandemic loans to federal SBA (cnbc.com)

Relevant excerpt: *The U.S. Secret Service returned $286 million in fraudulently obtained pandemic aid loans to the Small Business Administration, the agency announced Friday. The funds sent back to the SBA were obtained via the Economic Injury Disaster Loan (EIDL) program using both fabricated information and stolen identities.*

The suspects used Green Dot Bank, a fintech institution, to hold and move the fraudulent funds. More than 15,000 accounts were used in the conspiracy, by individuals in the U.S. as well as domestic and transnational organized crime rings, the agency said.

Source #5: Thomson Reuters, November 8, 2021: Transnational fraud exploits crises and technology to expand reach - Thomson Reuters Institute

Relevant excerpt: *Roy D. Dotson, Jr., a panelist, and Assistant Special Agent in Charge for the Jacksonville field office of the U.S. Secret Service, pointed to a specific date — March 27, 2020 — as standing out for him because that was the date the Coronavirus Aid, Relief and Economic Security (CARES) Act was signed into law, making "billions of dollars" available in pandemic relief. Almost immediately, fraudsters began submitting "millions, literally millions of fraudulent applications to both the state workforce agencies and to the Small Business Administration." Dotson noted the adage "fast money, fast crime" to describe the results. The need to get money out to people quickly and the overwhelming number of fraudulent applications, overwhelmed systems that were not able to keep up with identify verification it screens out the fraudsters.*

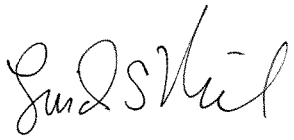
In addition to Marelli's' identification of China and other Asian countries as contributing to global fraud, Dotson included western African and Eastern European criminal enterprises that are active in cybercrime fraud.

Source #6: Government Accountability Office (GAO): Unemployment Insurance: DOL Needs to Address Substantial Pandemic UI Fraud and Reduce Persistent Risks

> **Relevant excerpt:** *According to National Association of State Workforce Agencies officials, the UI system faced unrelenting attacks by foreign organized crime groups during the pandemic.*

As is made clear by this reporting, the full extent of adversarial nations' participating in pandemic fraud is not yet known, but indications are that our adversaries played an extensive role in the theft of U.S. taxpayer dollars during and immediately following the pandemic.

Sincerely,



Linda Miller

CEO, Audient Group, LLC
Former Deputy Executive Director, Pandemic Response Accountability Committee

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

November 17, 2023

The Honorable David Schweikert
Chairman
Committee on Ways and Means
House of Representatives
Attention: Mr. Jonathan Kirk

Dear Mr. Chairman:

This letter responds to your request that we address questions submitted for the record related to the Committee's October 19, 2023, hearing entitled *Investigating Pandemic Fraud: Preventing History from Repeating Itself.* GAO's responses to these questions are enclosed.

If you have questions about this response or need additional information, please contact me at shear@gao.gov or at (202) 512-6722.

Sincerely yours,

Rebecca Shea

Rebecca Shea
Director, Forensic Audits and Investigative Service

Enclosure

House Committee on Ways and Means
Questions for the Record
Investigating Pandemic Fraud: Preventing History from Repeating Itself
October 19, 2023

1. What are existing tools that agencies can use to prevent money that is fraudulently claimed from going out the door?

A key tool that agencies can use to prevent the payment of fraudulently claimed funds is the Do Not Pay (DNP) working system operated by the Department of the Treasury. The DNP allows agencies to check various data sources for pre-award, pre-payment eligibility verification, at the time of payment and any time in the payment lifecycle. It allows them to verify eligibility of a vendor, grantee, loan recipient, or beneficiary. The service is available to agencies at no cost.

In addition, we and others have developed resources to help agencies strategically manage their fraud risks and enhance program integrity. These resources focus on preventing fraudulent and other improper payments.

- GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework), issued in July 2015. This framework provides a comprehensive set of key components and leading practices to help agency managers combat fraud in a strategic, risk-based way. The Fraud Risk Framework identifies a number of leading practices regarding the use of data analytic tools and techniques to prevent and detect fraud.

- GAO's Antifraud Resource, issued in January 2022, helps federal officials and the public better understand and combat federal fraud. The Antifraud Resource provides insight on fraud schemes that affect the federal government, their underlying concepts, and how to combat such fraud.

- GAO's *A Framework for Managing Improper Payments in Emergency Assistance Programs* (Managing Improper Payments Framework), issued in July 2023, is intended to help federal agencies mitigate improper payments, including those stemming from fraud, in emergency and nonemergency programs before they occur.

- Bureau of the Fiscal Service's Antifraud Playbook provides a how-to guide for implementing the Fraud Risk Framework's leading practices. The Playbook consists of a four-phased approach—aligned with the four components of the Fraud Risk Framework—and 16 best-practice plays for combatting fraud.

a. Do you see agencies using existing guardrails to the best of their ability? If not, how can Congress help incentivize agencies to use existing tools effectively?

We found that prior to the pandemic, federal agencies did not strategically manage fraud risks and were not adequately prepared to prevent fraud. We recognize that eliminating all fraud and fraud risk is not a realistic goal. However, a variety of resources and requirements for fraud risk management were in place well before the pandemic. Had agencies already been strategically managing their fraud risks, they would have been better positioned to

identify and respond to the heightened risks that emerged during the pandemic. Agencies have the opportunity to learn from the experiences during the pandemic and to ensure that they are strategically managing their fraud risks. Doing so by leveraging available resources and adhering to requirements will enable them to carry out their missions and better protect taxpayer dollars from fraud during normal operations and prepare them to face the next emergency.

We recently reported on certain factors that could strengthen agencies' efforts to manage fraud risks. Specifically, as we reported in *Fraud Risk Management: Agencies Should Continue Efforts to Implement Leading Practices* (GAO-24-106565), the 24 Chief Financial Officers Act of 1990 agencies indicated, in response to our survey, that the following factors are highly or somewhat motivating to increasing the maturity of their fraud risk management efforts:

- having congressionally directed prioritization of budget funds for program integrity improvements,
- having a provision of funds earmarked or appropriated for fraud risk management,
- ability to use a no-cost external resource for payment integrity checks or related support,
- general legislative requirements to do so,
- getting to keep identified recoveries (not returned to Treasury General fund), and
- having specific fraud risk management performance metrics or reporting requirements.

To help incentivize agencies to use existing tools effectively, we have suggested to Congress that it reinstate the requirement that agencies report on their antifraud controls and fraud risk management efforts in their annual financial reports. Such reporting will increase congressional oversight and focus agency attention to better ensure fraud prevention during normal operations and emergencies.

2. **Please provide details about the recommendations that the U.S. Government Accountability Office (GAO) has made to agencies within the federal government on ways to improve their COVID-19 pandemic fraud prevention, including whether the agencies agreed with these recommendations and the implementation status for each of the recommendations.**

GAO has made recommendations to agencies within the federal government on ways to improve their management of fraud risks in pandemic relief programs, including actions to prevent and detect fraud. This includes the 50 recommendations presented in Attachment 1. Of these recommendations, agencies have implemented 19 and partially addressed 6, while 25 remain open as not yet addressed.

3. **In August, the U.S. Attorney for the District of Maryland publicly credited his office prosecuting COVID-19 fraud as a reason for the drop in homicides and non-fatal shootings in Baltimore, Maryland. For example, the U.S. Attorney's office identified a man who used the same photo but different names on driver's licenses from five different states, debit cards, credit cards, and Social Security cards. The fraudster then used this information to file fraudulent Paycheck Protection Program (PPP) loan and unemployment insurance (UI) benefit applications for a total of $1.2 million. When the U.S. Attorney's office traced his activity and searched his home, they found guns purchased online with a fake alias, including one he had illegally modified into a machine gun. This shows that pandemic fraud has implications beyond financial**

harm to the federal government and taxpayers. Can you speak to the importance of the work prosecutors are doing on COVID-19 pandemic fraud, and how that might have a larger impact on preventing future crime?

Our analyses has shown that some of those charged by the Department of Justice (DOJ) with pandemic relief fraud are engaged in other criminal activities. Specifically, we found in *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs* that some fraud against the Paycheck Protection Program (PPP) and COVID-19 Economic Injury Disaster Loan (COVID-19 EIDL) program was allegedly perpetrated in conjunction with other crimes and by criminal groups.

- Of the 330 PPP and COVID-19 EIDL cases we identified as of December 31, 2021, 91 involved both programs, illustrating an effort to target multiple Small Business Administration (SBA) pandemic relief programs.
- In addition, in 46 of the 330 cases (14 percent) DOJ filed charges against individuals for defrauding other pandemic relief programs as well as PPP and COVID-19 EIDL. For example, in some cases associated with PPP and COVID-19 EIDL funds, individuals also allegedly defrauded state unemployment insurance (UI) programs or offered fraudulent COVID-19 tests or personal protective equipment.
- Our analysis further shows that 56 of 330 cases (17 percent) involved allegations of other crimes in addition to PPP and COVID-19 EIDL fraud, such as health insurance fraud, tax fraud, or romance scams.

Additionally, 10 PPP and COVID-19 EIDL cases involved criminal groups—which we define as domestic or international criminal organizations involved in illicit activity—that allegedly engaged in SBA pandemic relief fraud alongside other criminal activity. This includes criminal charges for trade-based money laundering, identity theft, and illegal gambling. For example:

- A fraudster applied for and obtained PPP and COVID-19 EIDL funds using shell companies that had no operations or employees. The applications falsely represented monthly payroll and gross income and included falsified tax forms. The fraudster applied for two PPP loans and obtained funds based on both applications, and also received funds based on one of eight COVID-19 EIDL advance applications. In total, the fraudster received $542,714 in PPP and COVID-19 EIDL funds, which were misused to purchase a BMW vehicle and a Rolex watch.

  At the same time, while obtaining small business relief funds, the fraudster received UI benefits claiming an active job search but inability to find employment. In 2020, the fraudster received $15,550 in UI benefits. The fraudster was sentenced to 2 years and 3 months in prison and 3 years of supervised release, as well as ordered to pay $542,714 in restitution for the PPP and COVID-19 EIDL fraud.

High incidence of fraud can lead to public perception that pandemic relief funds are easy to obtain fraudulently and make the government a target for further and future exploitation. As a result, the work of prosecutors related to COVID-19 pandemic fraud is important. According to DOJ officials, instances of fraud can normalize additional fraudulent behavior, which increases cynicism and leads the public to believe that "fraud happens all the time." The officials further emphasized that DOJ prosecutes fraud to restore faith in government by seeking justice, recovering stolen funds, and illustrating that the government holds bad actors accountable. As such, according to DOJ officials, most cases of pandemic relief fraud are publicized in press

releases to deter others from committing fraud and promote trust in government to prevent future crimes.

4. **On July 30, 2020, The U.S. Treasury Financial Crimes Enforcement Network published an advisory on Cybercrime and cyber-enabled crime exploiting the COVID-19 pandemic. The advisory contained descriptions of COVID-19 related malicious cyber activity and scams, associated financial red flag indicators, and information on reporting suspicious activity. Cyber-enabled schemes are continuing to drive pandemic fraud by allowing fraudsters to illegally obtain personal identifying information to fraudulently apply for COVID-19 pandemic benefits, including UI benefits. Please provide examples of large cyber-enabled COVID-19 pandemic fraud schemes that the GAO has examined.**

   During the course of our work, we have come across several examples of cyber-enabled COVID-19 pandemic fraud schemes. For example:

   - During the COVID-19 pandemic, a foreign national impersonated procurement officials of at least eight U.S. states and local governments and three educational institutions to fraudulently obtain medical equipment, such as defibrillators. He used a web hosting company to spoof state procurement email addresses and sought quotes for medical, laboratory, and computer equipment from targeted suppliers. The targeted suppliers were known to do business with the entities the foreign national was impersonating. The foreign national used the payment terms of "net 30 days", which is a standard term of trade credit for government and educational entities that requires payment for the goods within 30 days of delivery. He exploited this industry standard to fraudulently obtain equipment without providing any advance payment information or deposit prior to delivery of the equipment.

     Through this impersonation, the foreign national obtained and attempted to obtain millions of dollars of medical equipment, laboratory products, computer equipment and hardware, and other merchandise. This type of medical equipment, such as defibrillators, were in dire need during the COVID-19 pandemic because the high demand and stress on supply chains caused shortages and reduced accessibility to life-saving equipment. In February 2023, the foreign national pleaded guilty to wire fraud and was sentenced to more than 4 years in prison and ordered to pay more than $300,000 in restitution.

   According to Department of Labor (DOL) officials, the most common fraud schemes during the pandemic have included the use of stolen personally identifiable information (PII) to file an unemployment insurance (UI) claim or multiple claims; the use of synthetic identities (i.e., real identities mixed with fictitious information); and the use of bot attacks in attempts to overwhelm state UI systems or launch phishing schemes to obtain individual PII to perpetrate future fraud. DOL officials also told us that they have observed the use of new fraud schemes targeting CARES Act UI programs.

   - *Hijacking of bank accounts.* After an individual submits a legitimate application for UI benefits and provides bank account information for the funds' direct deposit, a fraudster will hack into the applicant's UI system account and reroute the deposit from the applicant's bank account to a bank account the fraudster can access.

   - *Mimicking of state UI websites.* When people conduct Internet searches for their state's UI office, they may find, and file claims on, a fraudulent website that looks like the state workforce agency's website, thus providing their PII to fraudsters.

Our analyses has shown that individuals were charged by DOJ with obtaining PPP and COVID-19 EIDL funds by stealing identities. We found in *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs* that these cases involved allegations of various types of identity theft. This involves the theft of personally identifiable and business information or the use of synthetic identities to obtain PPP and COVID-19 EIDL funds. Our analysis showed that as of December 31, 2021, 63 of the 330 PPP and COVID-19 EIDL cases (19 percent) involved allegations of theft of personally identifiable information and 17 cases (5 percent) involved allegations of using another business's information to obtain PPP or COVID-19 EIDL funds. Additionally, we identified 50 cases (15 percent) that involved Social Security Numbers (SSN) to apply for PPP and COVID-19 EIDL funds. Another 11 cases (3 percent) involved allegations of synthetic identity fraud where individuals fabricated an identity by using fictitious information in combination with stolen information such as an SSN.

Attachment 1: Selected COVID-19 Pandemic Fraud Prevention Recommendations to Federal Agencies, as of November 9, 2023

Agency or Program Office & Program or Activity of Recommendation	*Issued Report & Date*	*Recommendation*	*Agency Response*	*Recommendation Status as of November 9, 2023*
Small Business Administration – Paycheck Protection Program	Report: GAO-20-625: *COVID-19: Opportunities to Improve Federal Response and Recovery Efforts* Date: 6/25/2020	The Administrator of the Small Business Administration should develop and implement plans to identify and respond to risks in the Paycheck Protection Program to ensure program integrity, achieve program effectiveness, and address potential fraud, including in loans of $2 million or less.	Agency neither agreed nor disagreed	Closed – Implemented
Small Business Administration – Paycheck Protection Program	Report: GAO-21-387: *COVID-19: Sustained Federal Action is Crucial as Pandemic Enters its Second Year* Date: 3/31/2021	The Administrator of the Small Business Administration should conduct and document a fraud risk assessment for the Paycheck Protection Program.	Agency concurred/agreed	Closed – Implemented
Small Business Administration – Paycheck Protection Program	Report: GAO-21-387: *COVID-19: Sustained Federal Action is Crucial as Pandemic*	The Administrator of the Small Business Administration should develop a strategy that outlines specific actions to monitor and manage fraud	Agency concurred/agreed	Open – Partially Addressed

	Enters its Second Year Date: 3/31/2021	risks in the Paycheck Protection Program on a continuous basis.		
Small Business Administration – Economic Injury Disaster Loan Program	Report: GAO-21-265: *COVID-19: Critical Vaccine Distribution, Supply Chain, Program Integrity, and Other Challenges Require Focused Federal Attention* Date: 1/28/2021	The Administrator of the Small Business Administration should develop and implement portfolio-level data analytics across Economic Injury Disaster Loan program loans and advances made in response to COVID-19 as a means to detect potentially ineligible and fraudulent applications.	Agency neither agreed nor disagreed	Closed – Implemented
Small Business Administration – Economic Injury Disaster Loan Program	Report: GAO-21-387: *COVID-19: Sustained Federal Action is Crucial as Pandemic Enters its Second Year* Date: 3/31/2021	The Administrator of the Small Business Administration should conduct and document a fraud risk assessment for the Economic Injury Disaster Loan program.	Agency concurred/agreed	Closed – Implemented
Small Business Administration – Economic Injury Disaster Loan Program	Report: GAO-21-387: *COVID-19: Sustained Federal Action is Crucial as Pandemic Enters its Second Year* Date: 3/31/2021	The Administrator of the Small Business Administration should develop a strategy that outlines specific actions to address assessed fraud risks in the Economic Injury Disaster Loan program on a continuous basis.	Agency concurred/agreed	Open – Partially Addressed

Small Business Administration – Economic Injury Disaster Loan Program	Report: GAO-21-387: *COVID-19: Sustained Federal Action is Crucial as Pandemic Enters its Second Year* Date: 3/31/2021	The Administrator of the Small Business Administration should implement a comprehensive oversight plan to identify and respond to risks in the Economic Injury Disaster Loan program to help ensure program integrity, achieve program effectiveness, and address potential fraud.	Agency concurred/agreed	Closed - Implemented
Small Business Administration – Office of Capital Access – Restaurant Revitalization Fund	Report: GAO-22-105442: *Restaurant Revitalization Fund: Opportunities Exist to Improve Oversight* Date: 7/14/2022	The Associate Administrator for the Office of Capital Access should develop and implement data analytics across Restaurant Revitalization Fund awards as a means to detect potentially fraudulent award recipients.	Agency partially concurred/agreed	Closed – Implemented
Small Business Administration – Office of Capital Access – Restaurant Revitalization Fund	Report: GAO-22-105442: *Restaurant Revitalization Fund: Opportunities Exist to Improve Oversight* Date: 7/14/2022	The Associate Administrator for the Office of Capital Access should develop, document, and implement procedures to use enforcement data on suspected fraud in other Small Business Administration programs, such as Paycheck Protection Program, to identify	Agency did not concur/disagreed	Open – Not Addressed

		potential fraud in Restaurant Revitalization Fund recipients.		
Small Business Administration – Office of Capital Access – Restaurant Revitalization Fund	Report: GAO-22-105442: *Restaurant Revitalization Fund: Opportunities Exist to Improve Oversight* Date: 7/14/2022	The Associate Administrator for the Office of Capital Access should develop and implement a plan to respond to potentially fraudulent and ineligible Restaurant Revitalization Fund awards in a prompt and consistent manner. This plan should include coordinating with the Office of Inspector General to align efforts to address fraud.	Agency did not concur/disagreed	Open – Not Addressed
Small Business Administration – Office of Disaster Assistance – Shuttered Venue Operations Grant	Report: GAO-23-105199: *COVID Relief: SBA Could Improve Communications and Fraud Risk Monitoring for Its Arts and Entertainment Venues Grant Program* Date: 10/11/2022	The Associate Administrator of the Small Business Administration's Office of Disaster Assistance should ensure that its post-award monitoring procedures for the Shuttered Venue Operators Grant program specifically address the risks the agency has assessed, including fraud risks, and clearly link them to monitoring activities. As a part of this effort, the Small Business Administration	Agency partially concurred/agreed	Open – Not Addressed

		should document its tolerance for the risks it has identified.		
Small Business Administration – Fraud Risk Management Board	Report: GAO-23-105331: *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs* Date: 5/18/2023	The Administrator of the Small Business Administration, in coordination with the Fraud Risk Management Board, should ensure that the Small Business Administration has mechanisms in place and utilizes them to facilitate cross-program data analytics.	Agency concurred/agreed	Open – Not Addressed
Small Business Administration – Fraud Risk Management Board	Report: GAO-23-105331: *COVID Relief: Fraud Schemes and Indicators in SBA Pandemic Programs* Date: 5/18/2023	The Administrator of the Small Business Administration, in coordination with the Fraud Risk Management Board, should ensure that the Small Business Administration has identified external sources of data that can facilitate the verification of applicant information and the detection of potential fraud across its programs. It should then develop a plan for obtaining access to those sources, which may involve pursuing statutory authority or entering into data-sharing	Agency concurred/agreed	Open – Not Addressed

		agreement to obtain such access.		
Department of Health and Human Services – COVID-19 Uninsured Program	Report: GAO-21-387: *COVID-19: Sustained Federal Action is Crucial as Pandemic Enters its Second Year* Date: 3/31/2021	The Secretary of Health and Human Services should finalize and implement a post-payment review process to validate COVID-19 Uninsured Program claims and to help ensure timely identification of improper payments, including those resulting from potential fraudulent activity, and recovery of overpayments.	Agency concurred/agreed	Closed – Implemented
Department of Housing and Urban Development – Office of the Chief Financial Officer and HUD Cares Act Compliance Response Team –CARES Act funds	Report: GAO-21-104542: *COVID-19: Additional Risk Assessment Actions Could Improve HUD Oversight of CARES Act Funds* Date: 9/30/2021	The Office of the Chief Financial Officer and the HUD CARES Act Compliance Response Team should work with relevant program offices to identify inherent or new fraud risks, assess the program's fraud risk tolerance, document the program's fraud risk profile, and take appropriate action to mitigate identified potential risks for each of the six CARES Act-funded programs that meet the front-end risk assessment criteria.	Agency concurred/agreed	Open – Not Addressed

Department of Housing and Urban Development – CARES Act funds	Report: GAO-21-104542: *COVID-19: Additional Risk Assessment Actions Could Improve HUD Oversight of CARES Act Funds* Date: 9/30/2021	The Office of the Chief Financial Officer and the HUD CARES Act Compliance Response Team should work with relevant program offices for each of the six CARES Act programs that meet the Department of Housing and Urban Development's front-end risk assessment criteria to reassess the need to either (1) conduct a full front-end risk assessment; or (2) take and document additional risk assessment steps to align with key aspects of the front-end risk assessment process, such as ranking risks and developing plans to mitigate identified risks.	Agency did not concur/agree	Open – Not Addressed
Department of Labor – Small Business Administration's Paycheck Protection Program	Report: GAO-20-625: *COVID-19: Opportunities to Improve Federal Response and Recovery Efforts* Date: 6/25/2020	The Secretary of Labor should, in consultation with the Small Business Administration and the Department of the Treasury, immediately provide information to state unemployment agencies that specifically addresses the Small Business Administration's	Agency neither agreed nor disagreed	Closed - Implemented

		Paycheck Protection Program loans, and the risk of improper payments associated with these loans.		
Department of Labor – Unemployment Insurance	Report: GAO-22-105051: *COVID-19: Additional Actions Needed to Improve Accountability and Program Effectiveness of Federal Response* Date: 10/27/2021	The Secretary of Labor should designate a dedicated entity and document its responsibilities for managing the process of assessing fraud risks to the unemployment insurance program, consistent with leading practices as provided in our Fraud Risk Framework. This entity should have, among other things, clearly defined and documented responsibilities and authority for managing fraud risk assessments and for facilitating communication among stakeholders regarding fraud-related issues.	Agency neither agreed nor disagreed	Open – Partially Addressed
Department of Labor – Unemployment Insurance	Report: GAO-22-105051: *COVID-19: Additional Actions Needed to Improve Accountability and Program Effectiveness of*	The Secretary of Labor should identify inherent fraud risks facing the unemployment insurance program.	Agency neither agreed nor disagreed	Closed – Implemented

	Federal Response Date: 10/27/2021			
Department of Labor – Unemployment Insurance	Report: GAO-22-105051: *COVID-19: Additional Actions Needed to Improve Accountability and Program Effectiveness of Federal Response* Date: 10/27/2021	The Secretary of Labor should assess the likelihood and impact of inherent fraud risks facing the unemployment insurance program.	Agency neither agreed nor disagreed	Closed – Implemented
Department of Labor – Unemployment Insurance	Report: GAO-22-105051: *COVID-19: Additional Actions Needed to Improve Accountability and Program Effectiveness of Federal Response* Date: 10/27/2021	The Secretary of Labor should determine fraud risk tolerance for the unemployment insurance program.	Agency neither agreed nor disagreed	Open – Not Addressed
Department of Labor – Unemployment Insurance	Report: GAO-22-105051: *COVID-19: Additional Actions Needed to Improve Accountability and Program Effectiveness of Federal Response*	The Secretary of Labor should examine the suitability of existing fraud controls in the unemployment insurance program and prioritize residual fraud risks.	Agency neither agreed nor disagreed	Closed – Implemented

	Date: 10/27/2021			
Department of Labor – Unemployment Insurance	Report: GAO-22-105051: *COVID-19: Additional Actions Needed to Improve Accountability and Program Effectiveness of Federal Response* Date: 10/27/2021	The Secretary of Labor should document the fraud risk profile for the unemployment insurance program.	Agency neither agreed nor disagreed	Closed – Implemented
Department of Labor – Unemployment Insurance	Report: GAO-23-105523: *Unemployment Insurance: Data Indicate Substantial Levels of Fraud during the Pandemic; DOL Should Implement an Antifraud Strategy* Date: 12/22/2022	The Secretary of Labor should design and implement an antifraud strategy for unemployment insurance based on a fraud risk profile consistent with leading practices as provided in the Fraud Risk Framework.	Agency partially concurred/agreed	Open – Partially Addressed
Department of the Treasury – Emergency Rental Assistance Program	Report: GAO-22-105490: *Emergency Rental Assistance: Additional Grantee Monitoring Needed to Manage Known Risks*	The Secretary of the Treasury, in consultation with the Treasury Inspector General, should develop and implement procedures to monitor and evaluate Emergency Rental Assistance grantees' controls,	Agency neither agreed nor disagreed	Open – Not Addressed

	Date: 2/10/2022	including through the reallocation process. The monitoring procedures should include information on the minimum internal control systems expected for Emergency Rental Assistance grantees that rely on self-attestation and other administrative flexibilities that could increase risks of improper payments.		
Department of the Treasury – Homeowner Assistance Fund	Report: GAO-22-105397: *COVID-19: Current and Future Federal Preparedness Requires Fixes to Improve Health Data and Address Improper Payments* Date: 4/27/2022	The Secretary of the Treasury should develop and implement written procedures to monitor Homeowner Assistance Fund participants' programs and uses of funds for compliance with program requirements and improper payments.	Agency concurred/agreed	Open – partially addressed
Department of Homeland Security – Federal Emergency Management Agency's COVID-19 Funeral Assistance	Report: GAO-22-105397: *COVID-19: Current and Future Federal Preparedness Requires Fixes to Improve Health Data and Address Improper Payments* Date: 4/27/2022	The Federal Emergency Management Agency Administrator should address deficiencies in the COVID-19 Funeral Assistance data by updating data records as data are verified, and adding data fields where necessary, to ensure that consistent and	Agency concurred/agreed	Open – Partially Addressed

		accurate data are available for monitoring of potential fraud trends and identifying control deficiencies.		
Department of Homeland Security – Federal Emergency Management Agency's COVID-19 Funeral Assistance	Report: GAO-22-105397: *COVID-19: Current and Future Federal Preparedness Requires Fixes to Improve Health Data and Address Improper Payments* Date: 4/27/2022	The Federal Emergency Management Agency Administrator should take action to identify the causes of the gaps in internal control in COVID-19 Funeral Assistance and design and implement additional control activities, where needed, to prevent and detect improper payments and potential fraud.	Agency concurred/agreed	Closed - Implemented
US Department of Agriculture – Coronavirus Food Assistance Program	Report: GAO-22-104397: *Coronavirus Food Assistance Program: USDA Should Conduct More Rigorous Reviews of Payments to Producers* Date: 9/8/2022	The Administrator of the Farm Service Agency should direct agency officials conducting the Coronavirus Food Assistance Program payment spot checks to (1) use support generated by third parties; or (2) if such support is not available, document why support self-generated by the producer was accepted.	Agency generally concurred/agreed	Closed – Implemented

US Department of Agriculture – Coronavirus Food Assistance Program	Report: GAO-22-104397: *Coronavirus Food Assistance Program: USDA Should Conduct More Rigorous Reviews of Payments to Producers* Date: 9/8/2022	The Administrator of the Farm Service Agency should conduct additional spot checks of the Coronavirus Food Assistance Program payments and use a more risk-based approach to selecting procedures for review. This approach could include focusing on producers of commodities not generally covered by other Farm Service Agency programs and producers that received large payments.	Agency generally concurred/agreed	Open – Not Addressed
US Department of Agriculture – Coronavirus Food Assistance Program	Report: GAO-22-104397: *Coronavirus Food Assistance Program: USDA Should Conduct More Rigorous Reviews of Payments to Producers* Date: 9/8/2022	The Administrator of the Farm Service Agency should direct state offices to monitor the quality of the county offices' spot checks for the Coronavirus Food Assistance Program. Such monitoring could include a review of selected spot checks to ensure their accuracy.	Agency generally concurred/agreed	Closed – Implemented
US Department of Agriculture – Coronavirus Food Assistance Program	Report: GAO-22-104397: *Coronavirus Food Assistance Program: USDA Should Conduct*	The Administrator of the Farm Service Agency should issue guidance directing the agency to identify factors, such	Agency generally concurred/agreed	Closed – Implemented

	More Rigorous Reviews of Payments to Producers Date: 9/8/2022	as large claims for commodities with which the Farm Service Agency is unfamiliar, that county offices should consider when selecting procedures for the Coronavirus Food Assistance Program spot checks.		
Federal Communications Commission – Affordable Connectivity Program	Report: GAO-23-105399: *Affordable Broadband: FCC Could Improve Performance Goals and Measures, Consumer Outreach, and Fraud Risk Management* Date: 1/18/2023	The Office of the Managing Director should develop and implement a process, with clearly defined responsibilities and sources of information on fraud risks, for conducting fraud risk assessments for the Affordable Connectivity Program at regular intervals and when there are changes to the program or operating environment.	Agency concurred/agreed	Closed – Implemented
Federal Communications Commission – Affordable Connectivity Program	Report: GAO-23-105399: *Affordable Broadband: FCC Could Improve Performance Goals and Measures, Consumer Outreach, and Fraud Risk Management*	The Office of the Managing Director should develop and implement an antifraud strategy for the Affordable Connectivity Program that aligns with leading practices in the Fraud Risk Framework. These practices include documenting and	Agency concurred/agreed	Closed – Implemented

	Date: 1/18/2023	communicating the program's activities for preventing, detecting, and responding to fraud and establishing roles and responsibilities of those involved in fraud risk management activities.		
Federal Communications Commission – Affordable Connectivity Program	Report: GAO-23-105399: *Affordable Broadband: FCC Could Improve Performance Goals and Measures, Consumer Outreach, and Fraud Risk Management* Date: 1/18/2023	The Office of the Managing Director should develop and implement processes to monitor antifraud controls related to preventing duplicate subscribers in the Affordable Connectivity Program.	Agency concurred/agreed	Open – Not Addressed
Federal Communications Commission – Affordable Connectivity Program	Report: GAO-23-105399: *Affordable Broadband: FCC Could Improve Performance Goals and Measures, Consumer Outreach, and Fraud Risk Management* Date: 1/18/2023	The Office of the Managing Director should develop and implement processes to monitor antifraud controls related to subscriber identify verification in the Affordable Connectivity Program.	Agency concurred/agreed	Closed – Implemented
Federal Communications	Report: GAO-23-105399:	The Office of the Managing Director	Agency concurred/agreed	Open – Not Addressed

Commission – Affordable Connectivity Program	*Affordable Broadband: FCC Could Improve Performance Goals and Measures, Consumer Outreach, and Fraud Risk Management* Date: 1/18/2023	should develop and implement processes to monitor antifraud controls related to subscriber address validation in the Affordable Connectivity Program.		
Federal Communications Commission – Affordable Connectivity Program	Report: GAO-23-105399: *Affordable Broadband: FCC Could Improve Performance Goals and Measures, Consumer Outreach, and Fraud Risk Management* Date: 1/18/2023	The Office of the Managing Director should use information obtained from monitoring processes to improve the design and implementation of fraud risk management activities in the Affordable Connectivity Program, including its fraud risk assessment and subsequent antifraud strategy.	Agency concurred/agreed	Open – Not Addressed
Department of Commerce – Tribal Broadband Connectivity Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance and Fraud Risk Needed for Tribal and Public-Private Partnership Grants*	For the Tribal Broadband Connectivity Program, the Administrator of the National Telecommunications and Information Administration should designate a dedicated entity to lead fraud risk management	Agency concurred/agreed	Open – Not Addressed

	Date: 1/24/2023	activities for the program.		
Department of Commerce – Tribal Broadband Connectivity Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance and Fraud Risk Needed for Tribal and Public-Private Partnership Grants* Date: 1/24/2023	For the Tribal Broadband Connectivity Program, the Administrator of the National Telecommunications and Information Administration should ensure that the dedicated entity identifies inherent fraud risks in the program.	Agency concurred/agreed	Open – Not Addressed
Department of Commerce – Tribal Broadband Connectivity Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance and Fraud Risk Needed for Tribal and Public-Private Partnership Grants* Date: 1/24/2023	For the Tribal Broadband Connectivity Program, the Administrator of the National Telecommunications and Information Administration should ensure that the dedicated entity assesses the likelihood and impact of inherent fraud risks in the program.	Agency concurred/agreed	Open – Not Addressed
Department of Commerce – Tribal Broadband Connectivity Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance and Fraud Risk Needed for Tribal and Public-Private*	For the Tribal Broadband Connectivity Program, the Administrator of the National Telecommunications and Information Administration should ensure that the dedicated entity	Agency concurred/agreed	Open – Not Addressed

	Partnership Grants Date: 1/24/2023	determines fraud risk tolerance for the program.		
Department of Commerce – Tribal Broadband Connectivity Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance and Fraud Risk Needed for Tribal and Public-Private Partnership Grants* Date: 1/24/2023	For the Tribal Broadband Connectivity Program, the Administrator of the National Telecommunications and Information Administration should ensure that the dedicated entity examines the suitability of existing antifraud controls in the program and prioritizes residual fraud risks.	Agency concurred/agreed	Open – Not Addressed
Department of Commerce – Tribal Broadband Connectivity Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance and Fraud Risk Needed for Tribal and Public-Private Partnership Grants* Date: 1/24/2023	For the Tribal Broadband Connectivity Program, the Administrator of the National Telecommunications and Information Administration should ensure that the dedicated entity documents the fraud risk profile for the program.	Agency concurred/agreed	Open – Not Addressed
Department of Commerce – Broadband Infrastructure Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance and Fraud Risk*	For the Broadband Infrastructure Program, the Administrator of the National Telecommunications and Information Administration	Agency concurred/agreed	Open – Not Addressed

	Needed for Tribal and Public-Private Partnership Grants Date: 1/24/2023	should designate a dedicated entity to lead fraud risk management activities for the program.		
Department of Commerce – Broadband Infrastructure Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance and Fraud Risk Needed for Tribal and Public-Private Partnership Grants* Date: 1/24/2023	For the Broadband Infrastructure Program, the Administrator of the National Telecommunications and Information Administration should ensure that the dedicated entity identifies inherent fraud risks in the program.	Agency concurred/agreed	Open – Not Addressed
Department of Commerce – Broadband Infrastructure Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance and Fraud Risk Needed for Tribal and Public-Private Partnership Grants* Date: 1/24/2023	For the Broadband Infrastructure Program, the Administrator of the National Telecommunications and Information Administration should ensure that the dedicated entity assesses the likelihood and impact of inherent fraud risks in the program.	Agency concurred/agreed	Open – Not Addressed
Department of Commerce – Broadband Infrastructure Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance*	For the Broadband Infrastructure Program, the Administrator of the National Telecommunications and Information	Agency concurred/agreed	Open – Not Addressed

	and Fraud Risk Needed for Tribal and Public-Private Partnership Grants Date: 1/24/2023	Administration should ensure that the dedicated entity determines fraud risk tolerance for the program.		
Department of Commerce – Broadband Infrastructure Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance and Fraud Risk Needed for Tribal and Public-Private Partnership Grants* Date: 1/24/2023	For the Broadband Infrastructure Program, the Administrator of the National Telecommunications and Information Administration should ensure that the dedicated entity examines the suitability of existing antifraud controls in the program and prioritizes residual fraud risks.	Agency concurred/agreed	Open – Not Addressed
Department of Commerce – Broadband Infrastructure Program	Report: GAO-23-105426: *Broadband Funding: Stronger Management of Performance and Fraud Risk Needed for Tribal and Public-Private Partnership Grants* Date: 1/24/2023	For the Broadband Infrastructure Program, the Administrator of the National Telecommunications and Information Administration should ensure that the dedicated entity documents the fraud risk profile for the program.	Agency concurred/agreed	Open – Not Addressed

PUBLIC SUBMISSIONS FOR THE RECORD

Nov 2, 2023

Statement for the Record before the U.S. House, Committee on Ways and Means, Subcommittee on Oversight on "Investigating Pandemic Fraud : Preventing History from Repeating Itself" (10.19)

Respectfully submitted on behalf of the Niskanen Center,

Matthew Darling, Senior Employment Policy Analyst

David Jimenez, Social Policy Government Affairs Manager

Will Raderman, Employment Policy Analyst

Chairman Schweikert, Ranking Member Pascrell, and Members of the Committee, thank you for conducting a critical recent hearing on pandemic fraud. Widespread fraud during the COVID-19 pandemic came at an enormous cost to the American taxpayer. The American people deserve social insurance systems that deliver critical assistance–including unemployment insurance (UI)–effectively and quickly to legitimate claimants.[1] Pervasive fraud costs taxpayers but also deepens cynicism in government. Without greater public confidence, lawmakers will be constrained in their ability to enact long overdue modernization of essential federal programs. Given the alarming gaps in UI integrity documented by government auditors and this Committee, Congress must strengthen the administration of UI and guard taxpayer dollars against fraud and criminal actors. Specifically, we encourage the Committee to explore opportunities to:

- Improve the quality of data sharing and coordination
- Foster professional cultures of institutional excellence in state agencies responsible for UI
- Fix long-standing gaps in adequate federal funding for state UI administration
- Encourage simplification of UI benefit calculation to limit fraud risks

Increase data sharing and coordination

Full use of national data platforms is crucial to minimizing fraudulent claims and maximizing efficiency. Government Accountability Office analysts have long recommended better information-sharing practices, but states have not taken advantage of all available options. It

[1] Shea, Rebecca. "COVID-19: Key Elements of Fraud Schemes and Actions to Better Prevent Fraud." Testimony before the Subcommittee on Oversight, Committee on Ways and Means, House of Representatives, October 19, 2023. United States Government Accountability Office. https://gop-waysandmeans.house.gov/wp-content/uploads/2023/10/Shea-Testimony-Updated.pdf.

was only in the wake of the COVID-19 pandemic that every state finally agreed to use the national Integrity Data Hub (IDH) for claim verification,[2] and many states still are not utilizing and supporting the full range of data services offered by the National Association of State Workforce Agencies.[3] For example, many states aren't participating in the multi-state cross-match platform; nor are they consistently providing claimant data to the IDH.[4] This is a missed opportunity to address significant sources of fraud during the pandemic.

The continued lack of participation by state UI programs in collaborative data efforts remains concerning. During the pandemic, multi-state claimants were the prevalent source of unemployment benefit fraud. State agencies were unable to communicate and share claims data effectively, leaving their programs vulnerable to criminals submitting applications in several locations.[5] Even when agencies managed to share their claims data, it could be incomplete or formatted differently from the information provided by other states. These dynamics must change to ensure that state UI programs are not vulnerable to similar levels of fraud moving forward and that more inadvertent improper payments stemming from clerical errors and incomplete paperwork are likewise avoided.[6]

Recommendations: Congress should consider mandating that states use critical data systems to maintain system integrity. Each data set that state agencies use is another layer of protection against criminal activity and improves the certainty that the correct number of dollars is going to the right people.

Additional ways to improve program performance and integrity should also be considered. For example, state programs could be provided access to centralized IRS data, as has been established with other federal agencies.[7] IRS data would equip UI agencies with a valuable

---

[2] U.S. Department of Labor, Employment and Training Administration. "Training and Employment Notice No. 24-21: Encouragement for States to Use the Integrity Data Hub (IDH) available through the Unemployment Insurance (UI) Integrity Center." May 5, 2022. https://www.dol.gov/sites/dolgov/files/ETA/advisories/TEN/2021/TEN_24-21_acc.pdf.

[3] National Association of State Workforce Agencies. "State Information Data Exchange System (SIDES)." Accessed October 24th, 2023. https://www.naswa.org/sides.

[4] Tian, Zhenying. "Integrity Data Hub: A Multi-State Solution to Unemployment Insurance Fraud." Bipartisan Policy Center, August 15, 2023. https://bipartisanpolicy.org/blog/integrity-data-hub-multi-state-solution-unemployment-insurance-fraud/.

[5] Darling, Matt. "What Star Wars can teach us about unemployment insurance fraud." Niskanen Center, April 11, 2023. https://niskanencenter.org/what-stars-wars-can-teach-us-about-unemployment-insurance-fraud/.

[6] U.S. Government Accountability Office. "UNEMPLOYMENT INSURANCE: Estimated Amount of Fraud during Pandemic Likely Between $100 Billion and $135 Billion." GAO-23-106696 Highlights, September 2023. https://www.gao.gov/assets/gao-23-106696-highlights.pdf.
U.S. Department of Labor. "PUA Improper Rate Report." August 21, 2023. https://oui.doleta.gov/unemploy/pdf/Pandemic_Unemployment_Assistance_Improper_Payment_Rate_Report.pdf.

[7] Esteban, Joanne, Nicole Fenton, and Christina Steen. "Federal tax data could streamline income verification and reduce fraud in future emergencies." U.S. Department of Labor, Employment and Training Administration. September 29, 2023. https://dol.gov/agencies/eta/ui-modernization/blogs/tax-data.

source of information to help verify claimants' identity and income from all possible sources and reduce time spent sifting through excessive paperwork.

Promote institutional excellence in state UI programs

The federal government must support state Departments of Labor (DOLs) as they strive for professional excellence and tackle inefficient and outdated practices. For example, New Jersey created a Cyber Fraud Investigations team to combat pandemic fraud. The state also modernized its system, putting workers at the forefront by ensuring they can easily navigate the UI website–demonstrating that anti-fraud efforts and effective benefits delivery work together.[8] Similarly, before the pandemic, Utah created a data warehouse designed "to monitor and evaluate possible fraudulent activity," leading to a historically low fraud rate in 2015.[9] This continued through the pandemic - from 2019 through 2022, Utah's "improper payment rate" was only 6.3%, the second lowest in the nation (the national average is 21.5%).[10] Concerned taxpayers and citizens should applaud reform-minded, ambitious state public sector leaders who independently pursue impact and accountability in their agencies.

Meaningful opportunities for federal engagement should also be a priority. While entrepreneurial state administrators have proactively improved their respective UI systems, others lack the necessary capacity or information. The federal government should continue highlighting promising practices that states can implement, conduct research on potential UI modernization efforts, and flag possible strategies to state agencies as has been done via the newly established Unemployment Insurance Office of Modernization.

Recommendations: Congress could consider authorizing and appropriating a Research and Development program that would evaluate, publicize, and support promising state initiatives on UI modernization, including anti-fraud efforts. The federal government should complement state innovations with an "ARPA-L" (Advanced Research Program - Labor), modeled after the successful "DARPA" program in the Department of Defense and the new "ARPA-H" program in Health and Human Services.[11] A vibrant federal-state partnership can help identify crucial UI reforms that ensure potential recipients can efficiently access their benefits while limiting fraud and overpayment risks.

---

[8] Evermore, Michele. "New Jersey's Worker-centered Approach to Improving the Administration of Unemployment Insurance." Heldrich Center for Workforce Development, Rutgers. September 2023. https://heldrich.rutgers.edu/sites/default/files/2023-09/New_Jersey_s_Worker-centered_Approach_to_Improving_the_Administration_of_Unemployment_Insurance.pdf.

[9] Newcombe, Tod. "Aiming Analytics at Our $3.5 Billion Unemployment Insurance Problem." Government Technology, March 2017. https://govtech.com/data/aiming-analytics-at-our-35-billion-unemployment-insurance-problem.html.

[10] U.S. Department of Labor, Employment and Training Administration. "Unemployment Insurance Payment Accuracy by State." Accessed October 23, 2023. https://dol.gov/agencies/eta/unemployment-insurance-payment-accuracy

[11] Schoop, Joshua, Arati Prabhakar, Jeff Kaplan, and Andrew Sosanya. "Creating an Advanced Research Projects Agency (ARPA-L) for the Department of Labor." Day One Project, March 2021. https://fas.org/wp-content/uploads/2021/03/Creating-an-Advanced-Research-Projects-Agency-ARPA-L-for-the-Department-of-Labor.pdf.

Identify sustainable funding streams for state UI administration

The administration of UI benefits (as well as employment services and other related capacities) is funded by the Federal Unemployment Tax Act (FUTA). FUTA is paid by the employer, with a rate of 6% on the first $7,000 of an employee's earnings. The $7,000 tax base was last updated in 1983, when the average worker's earnings were $313 a week (or $16,276 a year), and was applied to nearly half of the average worker's earnings. Today, weekly earnings have passed $1,000 a week (or $55,000 a year), so the FUTA tax is only applied to the first 13% of earnings.[12] Consequently, consistent annual funding for UI administration has consistently decreased.[13]

One-off increases to state funds, such as those appropriated during the COVID-19 pandemic, have temporarily made up some of this decline. Still, the lack of adequate long-term support to protect UI integrity remains deeply concerning. Take the development of information technology systems. In recent years, best practices in private sector software development (especially for complicated systems such as UI administration) have abandoned "waterfall" development processes (in which program development moves through a sequence of discrete stages, like a succession of waterfalls in a river). Now most private sector software companies use an "agile" development paradigm, in which the system is constantly being redeveloped and re-tested. "Agile" programs cannot be effectively financed with a system of one-off grants, but need consistent, steady financing to assure service continuation and eliminate "technical debt." As Jennifer Pahlka, the founder of "Code For America" and the U.S. Digital Service unit, has written, "Government's attachment to waterfall development seriously hinders its ability to build software that works well for the task at hand."[14] This is just one example illustrating the urgency of reliable, consistent funding for UI administration to protect taxpayer dollars from criminal fraud and UI overpayments.

Recommendations: Congress should provide states with consistent, sufficient funds to allow states to oversee their UI programs at high professional standards. Increasing the taxable earning base for FUTA would shore up resources for state UI administration and could be paired with greater simplification of how payroll taxes for Unemployment Insurance are applied to employers. Lawmakers could weigh pairing heightened federal investment in state UI administration with certain requirements, such as conducting certain types of verification checks for identity and earnings or setting aside a certain percentage of new dollars to focus solely on fraud prevention. Any mandates should be applied carefully so that state agency leaders

---

[12] "Employed Full Time: Median Usual Weekly Real Earnings: Wage and Salary Workers: 16 Years and Over." Federal Reserve Bank of St. Louis. Last modified October 18, 2023. https://fred.stlouisfed.org/series/LES1252881600Q.

[13] Wandner, Stephen A., ed. 2018. Unemployment Insurance Reform: Fixing a Broken System. Kalamazoo, MI: W.E. Upjohn Institute for Employment Research. https://doi.org/10.17848/9780880996532.

[14] Jennifer Pahlka, Recoding America: Why Government Is Failing in the Digital Age and How We Can Do Better (Henry Holt and Co., 2023)

maintain the necessary flexibility to invest in improvements to state DOLs that meet their specific challenges regarding staffing, benefit delivery, and program integrity.

Simplify UI benefit calculation to reduce fraud risks

We want to highlight a third issue that has received less attention but is critical to improving benefit delivery and preventing fraud: the inordinate complexity of how UI benefits are calculated.

States have substantial flexibility in determining the overall generosity of their UI benefits in both length of coverage and replacement of prior earnings. This is to be expected, as states have substantially different economies with stronger or more constrained tax bases.[15] While high-income states may be able to finance more expansive benefits, other states may not be able to without putting their economic growth and competitiveness at risk.

The state-to-state variability doesn't apply only to their benefits; rather, over time, each state has developed increasingly complex algorithms to determine UI benefits. As we explained in a recent white paper[16]:

"Consider, for example, the rules that govern the replacement rate–the amount of a worker's prior earnings that is replaced by UI benefits. Immense variation exists just in states that begin with "A":

- *Alabama looks at your earnings in the previous year by quarter. The state then averages the two quarters in which your wages were the highest and multiplies that by 1/26 to determine your weekly benefit.*
- *Alaska looks at your wages in the previous year. Your weekly benefit is set as a percentage of your annual wages, with the possible percentage ranging from 0.9 to 2.2 percent. In addition, your benefits are increased by $24 per dependent.*
- *Arizona looks at your highest-quarter wage (in the four-quarter "base period" before filing) and sets your weekly benefits to 1/25th of your wages in that quarter.*
- *Arkansas looks at the four previous quarters, takes the average wage, and multiplies that by 1/26.*

Rules in the other 46 states are similarly varied. States may use the highest quarter's wages for the previous year, average wages, or some combination of the two."

---

[15] Zhang, Jin, and Matt Darling. "A More Legible UI Policy." Niskanen Center. February 7, 2023. https://www.niskanencenter.org/a-more-legible-ui-policy/.

[16] Darling, Matthew, and Will Raderman. An Unemployment Insurance System That Works. Niskanen Center, September 2023. https://www.niskanencenter.org/an-unemployment-insurance-system-that-works-2/

This complexity is not necessarily related to the specific needs of workers in each state. Rather, it is a product of random drifts over time as legislators look to make UI benefits more or less generous. This complexity causes a ripple effect on UI fraud prevention.

First, convoluted UI benefit calculation limits states' capacity to quickly bolster their UI claims staff during emergencies and severe economic downturns. During the pandemic, normal hiring laws were suspended to allow states to hire temporary workers to assist with UI administration. The complexity of UI calculation meant that quickly-trained temporary workers often could not effectively and accurately assist in benefits administration, as the intricacies of state UI codes require significant expertise to understand and apply. This influx of temporary workers may have inadvertently increased the fraud and overpayment rate, even while improving benefit delivery speed.[17]

Second, simply managing the administration of a public benefit guided by highly complex formulas risks coming at the expense of management and staff attention to identifying and addressing signs of criminal fraud or widespread overpayments. Ultimately, variation in benefit calculation contributes to the larger complexity in the UI system that makes it difficult for federal and state authorities to collaborate and detect fraud.[18]

Recommendations: Congress should weigh UI reforms encouraging states to "clean up" their UI code. While states should have substantial flexibility in determining the aggregate generosity of their UI program, they should all work from a consistent system where each state effectively turns the dials of two or three variables up or down instead of the complex free-for-all of the current system. This measure would substantially simplify the cost of UI administration and make it more responsive to future economic shocks.

Conclusion

Although the magnitude of pandemic fraud was unprecedented, the administrative shortcomings that enabled such high levels of criminal activity have been apparent for years. After Hurricane Katrina, Louisiana and Mississippi faced a surge in unemployment benefit claims from residents impacted by the storm. Their UI agencies were unprepared to handle the increase in claims and were subsequently forced to ease up on the eligibility screening to quickly send benefits to

---

[17] Evermore, Michele, and Laura Valle Gutierrez. "The Pandemic and Unemployment Insurance Fraud." The Century Foundation, February 8, 2023. https://tcf.org/content/commentary/the-pandemic-and-unemployment-insurance-fraud/.

[18] U.S. Department of Labor, Office of Inspector General. "Alert Memorandum: Potentially Fraudulent Unemployment Insurance Payments in High-Risk Areas Increased to $45.6 Billion." September 21, 2022. https://oig.dol.gov/public/reports/oa/2022/19-22-005-03-315.pdf.

displaced workers.[19] The Department of Labor Inspector General later reported that the state programs essentially had "nonexistent" controls to verify eligibility.[20]

This institutional breakdown, while taking place during a different crisis fifteen years earlier, parallels the struggles faced by UI agencies during the pandemic. American taxpayers are counting on lawmakers to ensure their UI can withstand future crises and achieve two straightforward goals: protecting their hard-earned dollars from criminal fraud and getting resources quickly to vulnerable workers. Unless Congress proactively takes steps to improve UI administration, similar fundamental failures in program integrity will occur again.

---

[19] United States Government Accountability Office. "HURRICANES KATRINA AND RITA: Federal Actions Could Enhance Preparedness of Certain State-Administered Federal Support Programs." Report to Congressional Committees, February 2007. https://gao.gov/assets/gao-07-219.pdf.

[20] U.S. Department of Labor, Office of Inspector General. "Individuals Received Disaster Unemployment Assistance in Both Louisiana and Mississippi: Management Letter No. 06-06-010-03-315," September 29, 2006. https://oig.dol.gov/public/reports/oa/2006/06-06-010-03-315.pdf

November 2, 2023
<Sent via electronic mail>

The Honorable David Schweikert
Chairman, Oversight Subcommittee
United States House of Representatives
1100 Longworth Building
Washington, DC 20515
c/o WMSubmission@mail.house.gov

Dear Mr. Schweikert and Subcommittee Members,

As the only national organization singularly devoted to reducing welfare fraud for the last 50 years, the United Council on Welfare Fraud wants to commend the witnesses that testified before the Ways and Means Oversight Subcommittee Hearing on Pandemic Fraud on October 19, 2023, and add our voices to reinforce their powerful statements.

UCOWF is a national professional organization of investigators, administrators and claims and recovery specialists who are on the frontlines combating welfare fraud in the nation's public assistance programs. Our members come from across the country at the local, county and state level who work every day to protect the integrity the Supplemental Nutrition Assistance Program (SNAP), Medicaid, cash assistance and other social safety net programs and safeguard taxpayer resources.

Fraud, waste, and abuse make up the overwhelming majority of improper payments in government assistance programs. It is nothing new, yet the pandemic exposed the lack of common-sense oversight and accountability required to safeguard taxpayer funds and provided our nation's leaders with an opportunity to address this ongoing epidemic.

Linda Miller and Amy Simon, both seasoned and highly skilled experts, provided candid and forthright testimony, shedding light not only on the alarming extent of fraud during the pandemic but also on the ongoing exploitation of federal programs. Linda Miller and Amy Simon, both seasoned and highly skilled experts, provided candid and forthright testimony, shedding light not only on the alarming extent of fraud during the pandemic but also on the ongoing exploitation of federal programs.

In response to Congressman Schweikert's question, Linda Miller succinctly summarized the challenge posed by transnational criminals, stating, "*We've got a dynamic adversary, and we have very, very static processes that address them*." In the public assistance programs, the state and local agencies charged with distributing the benefits to the recipients are woefully unprepared to prevent fraud because these government agencies do not have access to basic technology to verify the identity of the applicant.

As Linda Miller aptly noted, government agencies that distribute public assistance benefits are bound by antiquated laws that prohibit the utilization of identity verification technology used in the private sector. Public assistance programs remain vulnerable and targeted by bad actors looking for easy profit and that did not end with the pandemic – history is continuing to repeat. The lack of identity verification for public assistance continues to cost taxpayers billions of dollars in SNAP alone.

For the last decade or more, there has been an ongoing debate within state and federal agencies about whether integrity should interfere with access to government benefits. UCOWF unequivocally asserts that integrity and access are not mutually exclusive but rather stand as separate and equally vital pillars.

We wholeheartedly endorse Amy Simon's testimony, both in her written submission and her oral presentation to the committee, which states, "*Suggesting that benefit timeliness and benefit accuracy must be opposing goals is a false dichotomy. Benefit timeliness for eligible claimants is often most possible when fraud attacks are identified and prevented. Eligible claimants and taxpayers pay a steep price when policymakers do not take fraud prevention, detection, investigation and/or prosecution as seriously as the circumstances warrant.*" Ms. Simon's insights are strikingly accurate, and her conclusions hold true for all federal assistance programs, including SNAP. We commend her insight and emphasize her statements.

Finally, we offer our support to the five key actions Linda Miller identified that Congress could take to prevent the recurrence of issues at hand. A commonality between all state and local agencies on the frontlines of detecting, preventing, and investigating fraud is they are understaffed, underfunded, and undervalued. The impact of having a dedicated fraud office with direct funding cannot be underestimated; it has the potential to drastically alter the current landscape, where state agencies grapple with under-resourced fraud detection units.

As you can see, we could break down each part of the witnesses' testimony and offer line-by-line support. We were exceedingly pleased to note that the witnesses provided information that aligns so closely to UCOWF's advocacy goals. We are unaware of any hearing that provided as much practical, real-world insights that promise to guide the development of methods and practices to aid investigators in their daily pursuit of identifying, preventing, and prosecuting welfare fraud.

We eagerly anticipate discussions on fraud and program integrity with all members of the Committee and Subcommittee and extend a warm invitation for any questions or comments. If you have any questions, please contact us at UCOWFmail@gmail.com.

Sincerely,

Carrol A. Christian

Carrol Christian
President
United Council on Welfare Fraud