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.

###