House Committee on Ways and Means, Work and Welfare Subcommittee

Testimony of Michele Evermore, Senior Fellow, National Academy of Social Insurance

March 5, 2026

Thank you, Chairman LaHood, Ranking Member Davis, and members of the committee for taking the time to examine this critical issue. Taxpayer dollars falling into the hands of criminals at the expense of people who are truly experiencing one of the most difficult times in their lives is something we all want to avoid. Worse, the fact that criminal crime rings have been involved means that money has been used for other nefarious purposes.

The prospect of an economic downturn is never "if," but "when." There is currently a great deal of crisis conversation around artificial intelligence (AI) and mass unemployment, which, to me, seems less certain than a mass layoff event caused by a variety of potential factors in the next few years. Having a functioning unemployment insurance system will be critical no matter the cause, but even more so if it is the kind of economy-restructuring event that technology may create. As we consider fraud detection and prevention, we should take into account the context of an economic downturn. We want the most accurate fraud efforts possible to ensure they remain in place during high-demand periods. States learned the hard lessons of the pandemic and have a foundation of high-tech fraud-fighting tools in place for the next downturn.

Fighting fraud in UI and other public benefit systems is important. A UI program lacking integrity – including both avoiding payments to ineligible individuals and ensuring timely payments to those who become eligible – becomes less effective as the macroeconomic stabilizer it was meant to be. This is a problem that every state takes seriously. Any effort to promote program integrity has to be approached with a steady seriousness that engages all stakeholders in good faith, including state agencies, legislatures, employers, claimants, vendors, financial institutions, and research organizations. Efforts that appear to be politically motivated cannot be met with the open, honest collaboration necessary to address such a serious and complicated issue. Communication with states when embarking on fraud recovery partnerships will be critical. To optimize collaboration, it should be clear from the federal government that it is acting in good faith on the goal everyone shares and comes to the table prepared to learn and provide actionable, cost-effective solutions. For example, the [U.S. Department of Labor's recent collaboration with the State of Maryland successfully resulted in $520 million dollars recovered](#).

The biggest challenge in considering any issue related to unemployment insurance is that there are 53 states, territories, and the District of Columbia, each with 53 entirely different ways of doing things. The definition of fraud varies, as does everything from monetary eligibility to good cause separations to something so basic as "week" or even "hour." How states detect and prevent fraud varies wildly, and how states are attacked by bad actors also varies considerably. As we discuss any particular lever for addressing fraud, we should do so by contextualizing the larger UI fraud situation and the much larger unemployment ecosystem, which I will detail in this testimony.

Unemployment Insurance context
In 1935, when the Social Security Act was passed, unemployment insurance was a broadly defined benefit. Dealing with mass unemployment brought on by the Great Depression, the program's goal was more than simply providing a weekly check to people involuntarily out of work. Unemployment provides countercyclical stabilization when workers have money to spend in the local economy. According to the IMF, [every additional dollar spent in unemployment benefits during economic downturns increases employment and boosts private sector earnings by more than $1.92](#). UI also keeps people attached to the workforce through weekly work search activities and through connection to employment and

reemployment services. It also prevents periods of unemployment from eroding worker wages and creating mismatches between workers' skills and their new jobs by providing claimants with a "reservation wage" that allows workers to seek a suitable replacement for their old job.

All employers are currently taxed a nominal Federal Unemployment Tax Act (FUTA) credit of 6 percent of the first $7,000 of each of their workers' pay, with 5.4 percent credited back if the state has an unemployment insurance system that meets very broad federal requirements. So, states are nominally taxed at $420 per employee per year, but only pay $42 unless their state has a long outstanding loan from the federal trust fund. The definition of a minimal qualifying program was largely set in 1935 with minor modifications over the years.

Prior testimony submitted to this subcommittee details why fraud spiked during the pandemic, but it is worth reiterating here that during the chaos of the pandemic, amidst the weak, existing UI infrastructure, criminals flocked to virtually every emergency program created to stabilize life in the US during COVID-19. Because UI has been in place for decades with very broad federal requirements, each state's system has evolved to work differently from others. Questions about optimal administration, program design, and eligibility standards are answered regularly in state legislatures and sometimes as often as daily in state agencies. UI programs are notoriously difficult to administer. In her book, *Recoding America: Why Government is Failing in the Digital Age and How We Can Do Better*, author Jennifer Pahlka talks about a California EDD worker who continually refers to himself as "the new guy," but when pressed on how long he'd been there, it was seventeen years. Still, he was less able to navigate the agency's challenging, ancient technology than his colleagues with 25 or more years on board.

In 2020, those antiquated systems met an entirely unexpected challenge. The first week of March, 211,000 initial claims were filed. Just two weeks later, nearly 3.3 million claims were filed. The highest on record prior to this was 695,000 in October of 1982. The last week of March 2020, 6.6 million people filed for unemployment, and 6.6 million more new claimants filed the week after that.

Also, in the last week of March 2020, Congress and the administration added three brand new programs that states needed to build quickly; Pandemic Unemployment Assistance (PUA) expanded eligibility, Federal Pandemic Unemployment Compensation (FPUC) added $600 and later $300 per week in benefits, and Pandemic Emergency Employment Compensation (PEUC) increase the number of weeks available for people who initially qualified for regular UI. States got new programs up and running in an average of 35 days. Over the course of the pandemic, Congress amended these programs twice. These programs were necessary because existing UI programs did not cover all workers who needed a benefit, replaced too little of prior income, and would not cover enough weeks to account for a global pandemic. At one point during the pandemic, about half of workers who got a benefit received it through PUA.

States also entered the pandemic with a 50-year low in administrative funding, and actually declining in real dollars by 23 percent.[i] Similarly, insufficient resources were provided to federal staff to support the U.S. DOL Office of Unemployment Insurance, the office tasked with providing extensive guidance, enforcement, assistance, and problem-solving during the pandemic. The enacted levels of funding for program administration in the area of workforce security, which funds UI program staff in the U.S. Department of Labor's national and regional offices, declined significantly, from a level of 419 full-time positions in FY 2006 to only 168 in FY 2021. States have also experienced high turnover since the start of the pandemic due to the extreme workload and harsh scrutiny they have faced.

Unemployment Insurance Administration
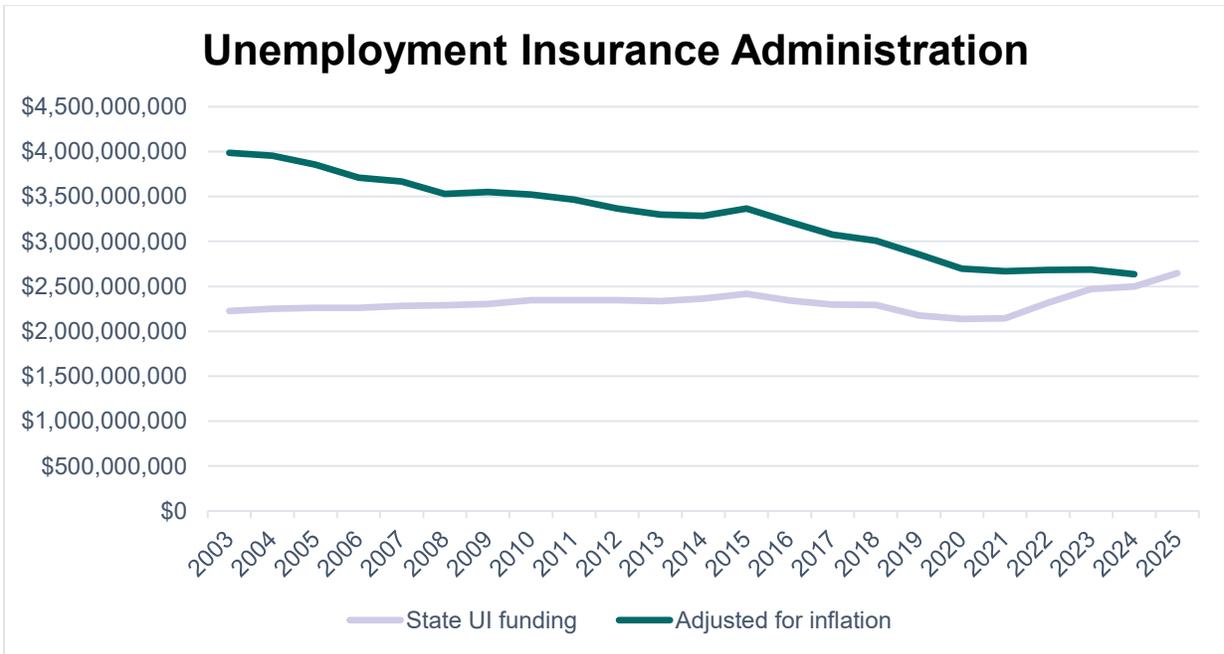
This extreme administrative challenge for states was worth it, because it helped to save lives, and the economy. More than [53 million people were able to access $870 billion](#) in benefits. This resulted in an astoundingly V-shaped recovery. As these payments made their way through the economy, the unemployment rate declined from 14.7 percent in April to 13.3 percent in May and 11.1 percent in June of 2020. The Federal Reserve found that the UI program was most effective on a dollar-for-dollar basis of any economic stimulus delivered during the pandemic.[1] Lacking a playbook for dealing with a situation as extreme as COVID-19, Congress and the administration sent unprecedented levels of support to a struggling workforce. Everyone knows someone who personally benefited from these programs, and those people haven't forgotten the effect it had on them during perhaps one of the most uncertain times in their lives.

Program integrity in the unemployment insurance context means paying the right people the right amount of money on time. Integrity efforts that hamper the other core goals of the program by not making timely payments or preventing legitimate claimants from accessing their earned benefit should not be considered to truly promote program integrity. States [continue to struggle with timely payment of benefits](#), so the right-sizing of fraud efforts continues to be an issue that states grapple with.

Using Debit Card Balances to Find Fraud
The Department of Labor Office of Inspector General (DOL OIG) has announced that it will be looking into bank card balances carrying unspent unemployment benefits to recoup payments to fraudsters. While I have some concerns about this, it is an area worth examining. It is true that fraudsters may have applied for benefits and had cards shipped to places where they could no longer retrieve them (such as infrequently used rental properties) or who are keeping debit card balances for some reason. However, balances may remain on some cards for a variety of legitimate reasons, such as a separate emergency fund, a claimant lost a card and had trouble navigating the process of replacing it, workers waited months to get their benefits and found new work by the time the card was issued and decided to save it for their next layoff, or needed car repair, or any variety of reasons. Some of the volume could simply be many cards with balances too small to be meaningfully used – a single dollar on enough cards still adds up. It is

---

important that those issues are taken into account. Given recent cuts to the Department of Labor's Office of Inspector General (DOL OIG) and overall staff loss at DOL, it will be important think carefully about allocating resources to fighting fraud. The DOL may therefore wish to concentrate more on detection and prevention than on this kind of recovery effort.

Congress should also be aware that, unless it extends statutory deadlines for fraud recoupment that have passed in the House, it could complicate these efforts. It should also be noted that between the first quarter of 2021 and the last quarter of 2025, $4.8 billion in overpayments has already been recouped,[ii] a testament to collaboration among states, the federal government, and financial institutions. In any fraud recovery effort, the return on investment for chasing previously paid fraud declines over time as cases grow colder.

One best practice to consider as this program rolls out is helping identity theft victims along the way. Most certainly, some of the fraud identified will be attached to someone whose identity was stolen. Notifying people whose identities were stolen about how they can protect themselves from further harm also helps prevent loss in other programs and the private sector, as these fraud rings do not confine themselves to unemployment. Fraud is not just a public benefits problem. According to the Financial Crimes Enforcement Network (FinCEN), banks experienced $212 billion in suspicious activity related to identity, which increased in 2023 to $394 billion in transactions.[iii] It is unfortunate that relatively small state unemployment programs are the first stop for well-organized and financed international crime rings, but some of them are already providing ID theft victims with good information to lock down their information. Connecticut's notice to ID theft victims is attached as an example of clear, simple notification of next steps, which is attachment 1 to this testimony. As I repeat throughout this testimony, there is no single tool or entity that can eliminate these crime syndicates on its own; all bodies and institutions that are potential targets must continue to collaborate closely.

Looking into debit card balances might not be the easiest or most accurate tool to recover fraud, as sophisticated crime rings likely have already consolidated balances elsewhere. This is also complicated because states have signed contracts with banks to pay funds that states have adjudicated to be paid, and so states will need to follow due process with the financial institutions and cardholders. The U.S. DOL has issued several guidance letters on recouping fraud from banks over the past few years.

Another issue to consider in this effort is that the relationship with the debit card issuer may not be in the same agency that has primary responsibility for unemployment insurance. For example, a state labor agency may house the unemployment insurance agencies that make eligibility determinations, but once that decision is made, benefit payments are turned over to a state treasurer, who then manages the contract with the debit card issuer. This will add some degree of complexity to the federal government's efforts.

As this and other fraud efforts move forward, it would make sense to engage with some kind of working group that includes a variety of states from all regions and other experts in fraud at national and state organizations, as well as within the vendor and financial services communities. There are several practical and legal considerations to take into account, and a good team working toward a shared goal will maximize the chance that this will result in real recovery or help to determine whether there might be more effective interventions. Naturally, this group should adhere to any federal advisory group laws and regulations.

Fraud vs. Overpayment
Before getting into overall fraud, it is important to distinguish fraud from overpayments. The vast majority of overpayments to claimants are mistakes, not crimes. The top two issues are almost always related to work search and benefit year earnings. The most recent program integrity reporting shows that 36 percent of overpayments were due to claimants not doing or misreporting work search, and 23.8 percent were due to misreporting earnings. Some portion of this overpayment rate is attributable to simple bad record-keeping.

The official reporting on overpayments is the Benefit Accuracy Measurement (BAM) program, which selects a limited number of cases and audits determinations. Both reporting work search and earnings is complicated. Many states do not require claimants to report their work search each week within the state system, but instead encourage workers to keep logs. Sometimes, when pressed by an auditor, claimants may not have details about all the work searches they have made in the past weeks because they did not write them down. Reporting earnings can be even more complicated. Many part-time workers have difficulty estimating how much they earn in a week until they see their paycheck, and whether they should factor in taxes and other deductions. Other workers simply confuse earnings with paychecks and report their payment when they receive it rather than when they earned it. Congress could dramatically reduce overpayments by standardizing work search and reporting, and allowing claimants to report payments rather than earnings.

**What States Are Doing – What is Working**
The National Academy of Social Insurance, in collaboration with the National Association of State Workforce Agencies (NASWA), and with support from Arnold Ventures, recently sent states an extensive 77-question survey about how they are working to detect and prevent fraud. Thirty-four states responded. A full report is forthcoming, but we are pleased to share some of our topline findings with the Ways and Means Committee today.

We promised states that, as a condition of participating in the survey, none of their individual responses would be made public and would only be used to better inform each other about efforts that work. However, we also promised to share anonymized findings that will help policymakers better understand the issue and how to go forward.

First, the good news is that fraud has declined, and in some states, to nearly zero. The bad news is that this does not mean states can relent on their efforts – fraud is only in decline due to steadily evolving responses to ever-changing criminal activity. States will never be able to return to a pre-2020 integrity stance. Fraud today is organized, automated, and increasingly AI-enabled. This is not residual pandemic disruption; it is the standing operating environment moving forward. States are now taking a robust, multi-layered approach to fraud detection and prevention. As of December 2024, the General Accountability Office (GAO), which rightly added the federal-state UI system to the high-risk list for several reasons ranging from inability to pay benefits on time to fraud exposure improved its outlook in terms of leadership and action plan, with improvements in capacity, monitoring, and progress.

UI Fraud Overpayments
June 2015 – June 2025
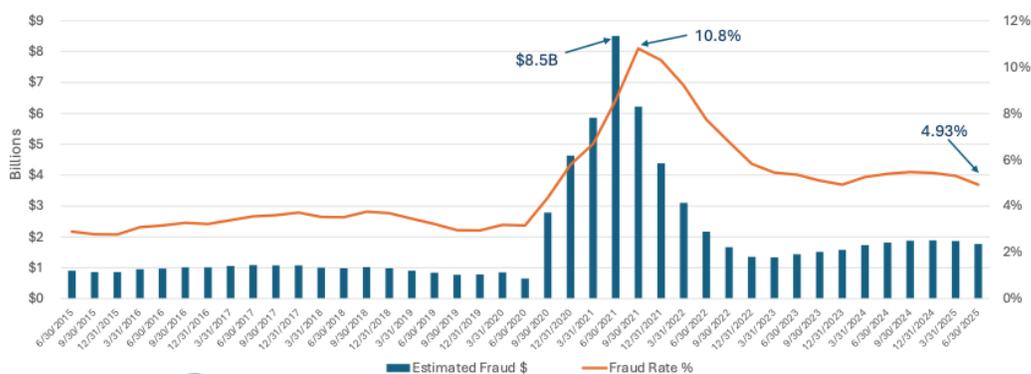
As repeated throughout this testimony, prevention is clearly the best place for resource-constrained states to focus their efforts. Recovery is important, and the 34 states responding to our survey reported more than $400 million in overpayments recovered in the last year. However, it is labor-intensive, legally complex, and often incomplete. Every dollar prevented before payment avoids downstream recovery costs and victim harm. The strongest return on state and federal investment comes from strengthening front-end prevention.

One of the more surprising findings is that, while there are some discernible trends, the face of fraud varies across states. States reported quite a bit of difference in the types of fraud committed and the schemes and characteristics of the fraudsters themselves. In some states, almost all fraud was organized crime, in others, it was all individual bad actors, and in most states, there was some combination of the two. Patterns that were more prevalent during the pandemic have abated, creating a more complex landscape.

We asked states how often they experienced various types of fraud. Given the prevalence of ID fraud, it would be reasonable to expect all states to report dealing with it on a daily basis; some states see this kind of fraud only on a monthly or yearly basis. Other types of fraud that at least several states commonly report include bank account takeover, fake employers, and claim takeover. Nearly every state reported expecting fraud attempts to increase over the next year, with several citing artificial intelligence (AI) as a growing concern. It would probably be helpful to think carefully about the threats AI might pose to all public and private systems in terms of fraud, and provide guidance to states to combat it.

I believe this committee would be pleased to learn the number of interventions and cross checks that states are already using. Every state responding to the survey is engaging with the federally funded Integrity Data Hub (IDH) administered by NASWA's UI Integrity Center, and the vast majority of states are fully using its functionality, including the Suspicious Actor Repository, Identity Verification, Bank Account Validation, Fraud Alert, Foreign IP Address, Suspicious Email Domains, Employer Data Module, and Do Not Pay. NASWA's addition of the Treasury Do Not Pay list has reportedly been of major help to states in terms of accurately flagging claims. All states also reported that they are using the State Information Data Exchange System (SIDES) except one, who said they are planning to begin using it this year. SIDES is a tool that helps streamline eligibility verification with employers. Most states reported that SIDES helped them pay benefits more quickly and accurately, but low employer participation is a challenge that states will need to address to fully utilize this tool.

On top of those tools, the vast majority of states are using a long list of cross-matching databases including, but not limited to:
- National Directory of New Hires (NDNH)
- Quarterly Wage Records
- Systematic Alien Verification for Entitlement (SAVE)
- State Directory of New Hires (SDNH)
- Social Security Administration Unemployment Insurance Query (SSA UIQ)
- Social Security Administration deceased person
- Interstate Connection Network (ICON)
- Prisoner Update Processing System (PUPS)
- Other incarceration databases (state, county, third party)
- State employee lists
- Department of Motor Vehicles (DMV), Driver's License
- Workers Compensation Crossmatch

When asked which of these crossmatches are the most useful to states, several responded that all of them are essential in fraud detection and prevention. Many states also responded that they plan to add more crossmatching functions in the future, including several products developed in-house.

Identity verification continues to evolve. All states have some kind of ID verification, but most have multiple methods, places in the process where ID re-verification may need to take place, and vendors to provide verification. As with other fraud prevention tools, states regularly review to ensure flagging accuracy. Most states provide ample alternatives for claimants who do not pass ID verification, but in some cases, claimants are unaware of those options or that their claim is being held for ID verification. I recommend that states offer as many off-ramps as possible, including in-person manual verification, a way to manually provide documents, a way to securely upload documents for review by the agency, and online video verification with a real person.

Identity Theft Fraud
12 Months – Sep 30, 2024
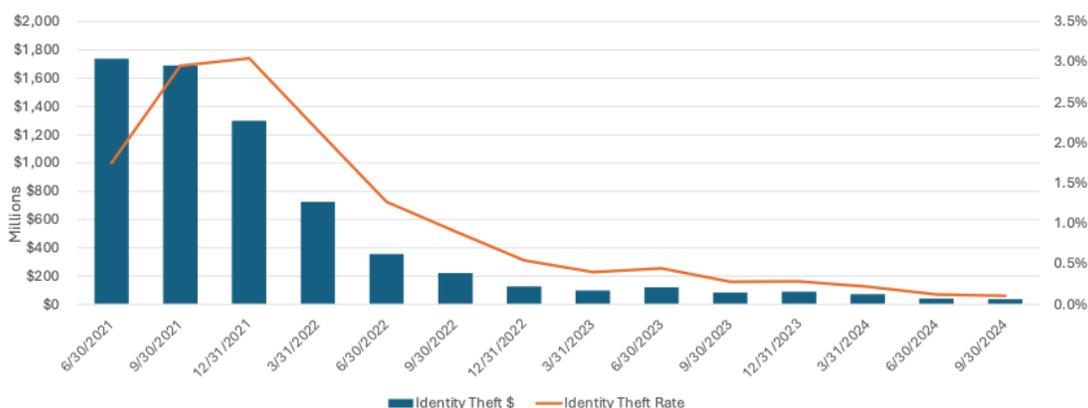
Consumers should be aware that fraudsters are using ever-evolving tactics to steal identities. One kind of false employer scam is even more nefarious than the usual creation of a false employer with the state to file for benefits – some fraudsters are creating false employers that claim to be hiring in order to get jobseekers to provide sensitive information. Scammers use romance schemes, engaging people on dating sites to gain personal information. They are texting claimants, pretending to be the state agency, and giving them a link to provide information so they can take over their accounts. Another helpful initiative would be public information campaigns to help people to understand fraudster tactics. This, again, would help with fraud outside the UI system, as well.

States are also employing modern technology barriers to fraudsters that are common in the private sector, such as requiring multi-factor authentication, using CAPTCHA, blocking international IP addresses, and other behind-the-scenes technology developed in-house. States have a far more sophisticated security posture than was necessary before 2020 – many of the in-house solutions states have developed are multi-prong and sophisticated.

Another efficiency to consider is testing and retesting the accuracy of fraud flags. One state reported that at one point in the past couple of years, half of initial claims were flagged and the vast majority of them were discovered to be legitimate claimants upon investigation. Another state reported that a quarter of its initial claims were flagged. Investigating and clearing these flags takes staff time and slows initial payment timeliness. States can work with vendors to understand what is causing flags. One state on the East Coast with a sizeable Puerto Rican population found that IP addresses from Puerto Rico would be flagged as a dangerous foreign IP, for example, when it might just be the case that someone who lost work went to stay with family in another US territory to save on expenses.

Another thing that could improve fraud rates is greater due process for those accused of fraud. Systems do make mistakes in identifying fraud. As most followers of UI recall, a faulty algorithm used by Michigan's MiDAS system determined more than 60,000 claimants committed fraud with a 93 percent error rate. While that is an extreme example, many states could add additional fact-finding steps to fraud determinations. Some states also have a narrow appeals window, such as within ten days of the decision being mailed. Clearing innocent claimants is a win/win for both states and the accused.

States identified several things that could help them on an ongoing basis. Better and more real-time data is an obvious way to continue to enhance efforts. Several states identified better education both to claimants and employers would reduce errors and speed determinations. States also cited a willingness and desire for additional collaboration with the federal government and other branches of state government. Another fairly great concern for states is an awareness of a potential mass layoff event in the future, and preparedness for such an event. Overall technology modernization is also a priority in several states – overall modernization is an integrity issue at least as much as it is for other priorities within agencies. However, the most consistently cited top issues are insufficient funding and staff to manage the workload.

Because states are now saddled with ongoing fraud detection and prevention, we should take that into account in funding models going forward. States have had to discontinue innovative prevention and detection projects as well as cancel contracts with fraud technology vendors as their funding allocated through the American Rescue Plan Act (ARPA) was rescinded. Over the past few years, however, an additional line item has been included in the administration's budget request and the final appropriation. This probably makes the most sense going forward, as well, as base funding to states is based on claims paid and fraud is somewhat separate from demand for the actual program. However, based on our survey, fraudsters are not targeting all states equally. Further research is necessary to better understand these patterns to allocate funding in the most efficient manner. Another potential source for funding fraud efforts has been proposed on a bipartisan basis: allowing states to retain a percentage of funds recovered.

Efforts that states are undertaking, which are being done primarily to serve other purposes, can also reduce improper payments. As noted above, most overpayments are mistakes. Poorly designed forms and technology can increase error rates, so as states make updates, consultation with integrity team members could help ensure that improvements in other areas help claimants avoid common mistakes.

Finally, I would be remiss in this testimony to not mention data security. Early in 2025, the Department of Government Efficiency (DOGE) accessed personally identifiable information (PII) associated with UI claims held by the DOL OIG, and then posted information about it on social media. DOGE has also been sharing Social Security data on an unsecured server. This is in addition to countless government-wide data security concerns raised about DOGE activity, including allegations of meddling with voter rolls. A proposed rule would expand DOL access to state UI data, to which I have commented with concerns that could create a single point of failure, potentially exposing the system to additional threats. DOL having greater insight into better data is not necessarily a bad thing, but going forward, the agency should adopt a stronger security posture than the administration has exhibited in 2025.

Closing
In closing, I want to recognize the hardworking state employees who work tirelessly to ensure the right people get benefits on time and safeguard state UI systems from fraud, as well as the federal workers partnering with them in good faith to keep our systems secure. At the end of the day, no algorithm or technology can fully replace seasoned government employees. In talking with state integrity officers over the years, they talk about the pride they take in getting more accurate every year, despite the challenges that arise, and the kind of resilience it takes to do this work. I urge Members of Congress to continue to engage the workers responsible for program integrity as it takes on the heady task of keeping UI systems secure now and into the future. [v]

---

[i] https://oui.doleta.gov/unemploy/pdf/transfplan/Building_Resilience_Complete%20document.pdf

NATIONAL ACADEMY
OF SOCIAL INSURANCE