Testimony of

JT Taylor
Senior Director of Fraud
ID.me, Inc.

"Reforming Unemployment Insurance to Support American Workers and Businesses"

United States House of Representatives
Ways and Means
Work & Welfare Subcommittee
June 4, 2024

ID.me is a Credential Service Provider (CSP) independently certified against the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3 Identity Assurance Level 2 (IAL2), and Authenticator Assurance Level 2 (AAL2). ID.me is able to verify users via omni-channel pathways, including Unsupervised Remote (online self-serve), Supervised Remote (video chat), and in-person options. ID.me supports over 129 million wallets and more than 650 customers, including 16 federal agencies and 40 state agencies across 30 states. Of the 129 million wallets, over 60 million have active NIST credentials.

JT Taylor
Senior Director of Fraud
ID.me

Chair LaHood, Ranking Member Davis, and distinguished committee members, thank you for the opportunity to testify today. I am honored to discuss "Reforming Unemployment Insurance to Support American Workers and Businesses." My name is J.T. Taylor, and I serve as the Senior Director of Fraud at ID.me. As I share insights and recommendations today, drawn from the breadth of my professional journey, I wish to highlight that these views are distinctly my own and may not necessarily align with the official positions of ID.me or affiliated entities.

Before this role, I dedicated over two decades to the U.S. Secret Service, the U.S. Intelligence Community, and the U.S. Military. These experiences provided me with a deep understanding of global security dynamics. As a Special Agent with the U.S. Secret Service, I led major domestic and international fraud and cybercrime investigations. My career in intelligence operations and investigative work has given me a comprehensive perspective on the complexities of digital fraud and cyber threats.

ID.me is a leading digital identity verification platform that protects consumers and businesses from fraud and identity theft. Our platform is designed to provide secure and convenient access to a wide range of services, ensuring that individuals' identities are verified accurately, efficiently, and in a privacy-enhancing way. ID.me serves over 129 million wallets, with over 60 million of these users holding a verified NIST IAL2 identity credential. This credential provides rapid access to essential services across various sectors, including government agencies, healthcare organizations, financial institutions, and consumer brands through the ID.me Digital Wallet.

We partner with numerous organizations in the private sector, as well as 16 Federal agencies and 40 state agencies across 30 states, to enhance security and streamline the identity verification processes. Our partnerships include collaborations with the U.S. Departments of Veterans Affairs, Treasury and dozens of state workforce agencies, among others. Our comprehensive approach and advanced technology have established ID.me as a trusted provider in the field of digital identity verification.

The CARES Act and Rampant Pandemic Fraud

The COVID-19 pandemic presented unprecedented economic challenges, requiring a swift response. In March 2020, the CARES Act was signed into law, designed to deliver emergency assistance to individuals and businesses affected by the pandemic. However, this rapid action opened the door to widespread fraud.

The extent of unemployment insurance (UI) and public assistance fraud during the COVID-19 pandemic has been a topic of significant debate, with various estimates highlighting the scale and impact of the issue.

In 2022, the Government Accountability Office (GAO) reported that the Federal government made improper payments totaling $247 billion, of which $200 billion were overpayments and excludes estimates for programs like the Pandemic Unemployment Assistance Program (PUA) and the Supplemental Nutrition Assistance Program (SNAP). This marks a distressing rise from $108 billion in 2012.[1] Recently, the GAO added another layer of complexity to the reporting, estimating pandemic-related UI fraud to be between $100 billion and $135 billion. The GAO's findings highlight the

[1]U. S. Government Accountability Office. Report (2023). Improper Payments: Fiscal Year 2022 Estimates and Opportunities for Improvement. March 29, 2023.

challenges in accurately quantifying fraud due to varying technological capabilities of state workforce agencies.[2]

ID.me estimates that overall figure to be higher and has publicly stated an estimated figure of $400 billion in fraudulent claims for unemployment insurance during the pandemic.[3] This is based on our unique vantage point of supporting 27 states simultaneously and synthesizing data and observations from across those states, including insights from multiple experts, analysts, and law enforcement officials. Cybersecurity professionals like Jon Coss and Rachel Greszler have also estimated that fraud could reach hundreds of billions of dollars nationwide.[4] Additionally, ID.me has substantial evidence of identity theft fraud that state audits may not detect, further supporting this estimate.[5]

Given the scale of improper payments and the technological limitations faced by many states, it is likely that it will take years to fully audit and uncover the extent of fraud during the pandemic.

These disparities in reporting stem from several factors:

- **Technological Limitations and Reporting Deficiencies:** Many states lacked the technological infrastructure to detect and report fraudulent claims accurately. For instance, the Department of Labor's (DOL) Inspector General (IG) reported that 60% of states did not complete the required reporting for fraudulent payments during the early months of the pandemic. This underreporting skews the overall fraud estimates, making it challenging to obtain a precise figure.

- **Varying Standards of Fraud Detection:** States differed in their ability to implement identity verification measures that could effectively detect and prevent fraud. States like Arizona and California, which adopted identity verification tools conforming to Department of Commerce's National Institute of Standards and Technology (NIST) standards early on, reported notable decreases in fraudulent claims. Conversely, states with slower implementation saw higher fraud rates, further complicating national estimates.

- **Scope of Identity Theft and Eligibility Fraud:** The introduction of new programs like PUA created new avenues for fraudsters. Eligibility fraud, where individuals applied for benefits in states where they were not eligible, compounded the problem. ID.me's data showed a peak in out-of-state applicants during the height of the pandemic, indicating widespread eligibility fraud that traditional state systems struggled to detect.

- **Organized Crime and International Fraud Rings:** The pandemic saw an influx of sophisticated fraud schemes orchestrated by domestic and international crime rings. The DOL IG and other experts have highlighted the role of organized crime in driving the surge in fraudulent claims, further inflating the estimated losses.

These various factors highlight the need for improved identity verification and reporting mechanisms. By understanding the complexities and challenges in reporting and detecting fraud, we can better appreciate the measures needed to reform the UI system, protect it from future exploitation, and ensure that those who need it most are able to access it. The vital process of digital identity verification, meant to ensure

[2] U.S. Government Accountability Office. Report (2023). Unemployment Insurance: Estimated amount of fraud during pandemic likely between $100 billion and $135 billion. September 12, 2023
[3] Hall, Blake. Calculating the Road to Losing $400 Billion Dollars. January 20, 2022.
[4] Greszler, Rachel. "Testimony before the Subcommittee on Financial Institutions and Consumer Protection Committee on Banking, Housing, and Urban Affairs." August 3, 2021.
[5] Podkul, Cezary. "How Unemployment Insurance Fraud Exploded During the Pandemic." ProPublica, July 26, 2021.

users – especially those applying for government benefits online – are genuinely who they claim to be, came under attack.

In the initial stages, urgency overshadowed the importance of accuracy and the integrity of the relief programs. Consequently, early initiatives were rolled out without mandating the verification of the claimant. Recognizing this potential vulnerability in the process, state-level benefits administrators stepped in, enforcing identity verification at diverse stages of the claims process. In the absence of rigorous identity verification for digital government services, the door was left wide open for identity theft and fraudulent claims.

From 2019 to 2020, the Federal Trade Commission saw a staggering 2,920% increase in identity theft reports associated with government document fraud. The post-pandemic period still witnesses rampant fraud, challenging our prevention systems. Despite the proven efficacy of the NIST identity assurance standards during the pandemic, some states opted for alternative solutions that do not adhere to NIST, resulting in a surge of fraud and numerous residents denied their rightful benefits. Notably, Ohio and Connecticut are still grappling with fraudulent and recurring onslaughts, illustrating the widespread and ongoing nature of this issue. At the same time, agencies within the Executive Branch are advancing the adoption of a National ID Verification Offering at the state level through direct subsidies and grants – even before it demonstrates the ability to meet the federal government's own standards.[6] We have seen what happens when states deploy non-conformant solutions and believe federal actions are exposing state agencies to a high – and avoidable – level of risk. Our nation faces a persistent and multifaceted threat from fraud, and concerted, coordinated efforts – with guidance and oversight from Congress – are required to address and rectify these vulnerabilities.

Interlinked Vulnerabilities

The pandemic brought about a monumental shift in global employment patterns, leading to an unparalleled rise in unemployment claims. Many states, faced with rapidly depleting unemployment reserves, turned to federal loans to ensure the continuation of benefit payouts. Notably, over twenty states took this route, creating a ripple effect that directly burdens the mainstays of our economy: small businesses.

The financing system supporting unemployment benefits is deeply integrated with the broader business ecosystem. Conventionally, businesses make contributions through a tax, calculated based on their workforce size, to support these benefit funds. However, with increasing state debts and evolving economic conditions, this once stable system is now in peril.

States grappling with significant budget deficits have considered reallocating funds initially set aside for mitigating these debts. As a result, the repayment responsibility is gradually being shifted onto businesses. This could mean that businesses, especially small ones, would face progressively increasing per-employee taxes each year for as long as this substantial debt remains—a period some analysts believe could extend up to a decade.[7]

Highlighting this situation emphasizes the critical relationship between the unemployment benefits system and the viability of small businesses. Fraud in unemployment programs doesn't just drain crucial funds; it indirectly threatens the very viability of business. Policymakers need to understand and address this

[6] Jones, John Hewett. FedScoop. GSA misled customer agencies over Login.gov privacy standard compliance, watchdog alleges. March 7, 2023; GSA GSA and DOL expand Login.gov partnership to increase access, decrease fraud, and support modernization in unemployment insurance. September 9, 2023.
[7] Ohanian, Lee. Hoover Institution. (n.d.). California defaults on $18.5 billion debt, leaving state businesses holding the bag. April 11, 2023.

intertwined challenge as Congress deliberates the path ahead. This issue will only worsen if states do not adopt or maintain strong digital identity verification standards.

During the peak of the pandemic, 27 states fortified their cybersecurity defenses by partnering with ID.me for digital identity verification. These states were under siege, facing relentless attacks from both nation-state adversaries and a mix of international and domestic fraudsters armed with vast troves of stolen identities. By integrating with ID.me and our NIST 800-63-3 compliant omni-channel solution, these states not only effectively curbed the majority of these fraudulent activities but also expedited the claim processing for genuine applicants. The impact was immense and quantifiable: several states have lauded ID.me for helping to prevent a staggering $273 billion in potential fraud losses.[8]

Common indicators of fraud emerged throughout the pandemic including questionable IP addresses, duplicative physical and email addresses, and the misuse of identification numbers. The volume and velocity of claims and applications made it challenging to establish rigorous checks and balances to mitigate fraud while ensuring timely claim processing for legitimate applicants in real time.

As we move beyond the pandemic's hardships, it is crucial to not overlook the insights these experiences have afforded us. As stewards of public funds and trust, federal and state agencies must refine their processes. Preparing for future emergencies requires developing more resilient, secure, and efficient systems to ensure assistance reaches those in need while minimizing the scope for misuse.

As former Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes, Elizabeth Rosenberg observed in January 2022, *"Rarely in public policy discussions do complex problems have simple solutions… But actually, there really is a kind of a silver bullet, at least one of the closest things to it that I've seen in public policy making–and that's digital ID… digital ID has the potential to immediately and dramatically improve how we protect our national security and our financial security.*

"Indeed, the adoption of such technological solutions can have a transformative effect. We've already witnessed this in action when states like Arizona, realizing the extent of fraud they were subjected to, collaborated with digital ID companies, such as ID.me. The results were profound: the introduction of this digital verification system acted as a deterrent, signaling to the fraudsters that their tactics were no longer viable."[9]

A critical oversight by agencies like the Small Business Administration (SBA) mirrored the challenges faced by the Department of Labor: they confused identity validation with identity verification. While validation merely ascertains that a combination of a Name, Date of Birth, and Social Security Number belongs to a real person, verification dives deeper, ensuring that the individual claiming an identity is indeed the rightful owner of that identity.

The vulnerabilities in relying exclusively on identity validation through personal identifiable information (PII) have been brutally exposed due to the plethora of data breaches.

---

[8] State of Arizona Department of Economic Security. "*Arizona Prevents More Than $75 Billion in Unemployment Benefit Fraud*."; McCarter, Mickey. *"Georgia Sought Identity Verification Solution to Stop Fraud."* State Tech Magazine, October 13, 2021; State of California, Office of Governor Gavin Newsom. "*EDD Recovers $1.1 Billion in Unemployment Insurance Funds, with More Investigations and Recoveries to Come*" June 21, 2022; Kanowitz, Stephanie. Route Fifty "*UI modernization, identity verification limit state fraud loss.*" March 20, 2023; State of Nevada, Department of Employment, Training and Rehabilitation (DETR). "*Director Elisa Cafferata announces resignation from the Department of Employment, Training and Rehabilitation (DETR)*" December 23, 2022; State of New Jersey, Department of Labor & Workforce Development. *"NJDOL Looks Back at 2021 Accomplishments While Continuing to Aid Workers, Businesses Amid Ongoing Global Pandemic."* January 3, 2022.

[9] Elizabeth Rosenberg, Assistant Secretary for Terrorist Financing and Financial Crimes, U.S. Treasury. Better Identity Coalition "Identity, Authentication, and the Road Ahead" January 24, 2022.

An alarming instance was in 2017 when the Chinese People's Liberation Army purportedly pilfered the Equifax database, compromising the sensitive personal information of roughly 150 million American adults. With such an expansive stolen database containing names, dates of birth, and SSNs, fraudsters found it easy to deceitfully claim pandemic assistance in systems relying solely on identity validation by simply fabricating their employment records.

A telling account from USA Today highlighted the simplicity of this fraudulent exercise. They interviewed a university student in Africa who candidly shared his modus operandi: by spending just $2 on the dark web, he could purchase stolen identities and file deceptive claims. His strike rate was profitable, managing a successful fraudulent payout for roughly one in every six attempts. His return on investment? A staggering profit, turning an initial outlay of $12 into a fraudulent windfall of $50,000.[10]

Robust identity verification methods like the IAL2 standard could have significantly reduced the fraud experienced during the pandemic. Not only would these standards have been instrumental in curbing malicious activities, but they could also have been leveraged to implement enhanced controls to thwart social engineering attempts. Moreover, beyond the obvious advantage of fraud prevention, a uniform embrace of these standards paves the way for enhanced interoperability across federal and state agencies. This, in turn, would lead to a more streamlined and positive experience for Americans.

Data Brokers Amplify Vulnerabilities: How Third-Party Data Compromises Intensify Fraud in Federal Benefit Programs

The thriving realm of data brokers has emerged as a potential pitfall in the seamless execution of various state and federal benefits delivery efforts, particularly in the backdrop of the COVID-19 crisis. Through my research and experiences on this subject, a glaring issue became apparent: hacked accounts from consumer data brokers became potent tools in fraudulent activities. Not only did they aid in bogus COVID-19 related business loans, but also fueled counterfeit unemployment claims.

In mid-2020, renowned cyber-security watchdog KrebsOnSecurity unveiled concerning findings. An informant, seeking anonymity, revealed an alarming trend: a network of fraudsters was rampantly disseminating intricate personal and financial data of Americans.[11] Even more unsettling was the discovery that the data had its roots in a U.S.-based consumer data broker. Investigations unveiled that this analytics giant had been compromised, feeding these fraudsters with invaluable consumer data.

The information trafficked by these scammers is no ordinary data. It encapsulates everything from full Social Security numbers to personal addresses, and even to granular details like IP addresses tied to a consumer's online activities. What made this even more disturbing was the sheer extent and depth of the data being funneled. The compromised data wasn't just aiding identity theft; it was facilitating multi-state unemployment claims and fraudulent loan applications.

Historical data serves as a testimony to the recurrent misuse of consumer data. In 2013, a startling revelation saw a 24-year-old operating an identity theft service from Vietnam, granting unauthorized access to the personal and financial data of over 200 million Americans. This breach was orchestrated by deceitfully posing as a private investigator to a subsidiary of a major credit bureau.[12] Such instances expose the deep-seated vulnerabilities of data brokers and their consequential impact.

---

[10] Penzenstadler, Nick. USA Today. How scammers siphoned $36B in fraudulent unemployment payments from US. December 30, 2020.
[11] Krebs, B. KrebsOnSecurity. Hacked Data Broker Accounts Fueled Phony COVID Loans, Unemployment Claims. Krebs on Security. August 21, 2020.
[12] Krebs, B. Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records. Krebs on Security. March 10, 2024.

While major credit bureaus remain pivotal, Nicholas Weaver, a distinguished academic from UC Berkeley, suggests that data brokers could be the bigger goldmine for ID thieves. This is primarily because of the breadth and depth of the information they hold, which goes beyond static identifiers like SSNs. It's comprehensive enough for knowledge-based authentication – a primary requirement for credit validations, and a practice that has been recommended by experts to be retired because of its ineffectiveness in preventing fraud.

Fraudsters often cash out using money mules, cryptocurrency, prepaid cards, or online-only banks, allowing for substantial transaction amounts. These instruments allowed for substantial transaction amounts, making them especially attractive for fraudulent activities. One can't help but concur with Justin Sherman's recent observation to the House Energy and Commerce Committee that the current debate on consumer consent is "broken."[13] The convoluted labyrinth of terms of service agreements, filled with jargon and legalese, effectively ensures that users are unaware of the rights they're signing away. This is not genuine consent but an orchestrated obfuscation of the truth.

Furthermore, while recent FTC actions and penalties against data brokers are commendable, sporadic enforcement is hardly a sustainable solution. The industry's rapid growth, coupled with the complexity of digital ecosystems, necessitates comprehensive and systemic solutions. As FTC Commissioner Rebecca Kelly Slaughter aptly noted, individual enforcement actions can only do so much. It is up to Congress to enact robust, holistic regulations that protect individual privacy rights while ensuring data brokers operate within well-defined, ethical bounds.[14] The era of unchecked data brokerage needs stringent oversight. A balance must be struck between the data-driven digital economy and the inviolable right to privacy. The American people deserve nothing less.

Inclusivity and Accessibility in Identity Verification

Ensuring that federal and state agencies are sufficiently equipped to tackle identity-based fraud should not mean a compromise on accessibility. This balance is essential to maintaining inclusivity, privacy and fairness in identity verification processes. Legacy methods of identity verification, powered by data brokers and credit bureaus, struggle to verify users without a presence in online records, which are primarily comprised of financial records. These legacy methods – still in place across federal and state agencies today – link access to affluence. Their use disadvantages lower-income users, which disproportionately impacts the young and minorities. Consumer Financial Protection Bureau estimates there are 45 million Americans who have “invisible,” incorrect, or unscorable credit.[15] These are users that would likely have been unable to verify their identity using legacy methods.

ID.me’s NIST 800-63-3 compliant omni-channel solution is designed to help these and other underserved populations that have traditionally struggled to verify their identity online: low-income users, veterans living overseas, individuals with recent name changes, and individuals with housing insecurity. In doing so, we close about 75% of the digital divide left by algorithm-only solutions by offering users alternative pathways to verification. We are also the only provider in the market that provides alternatives for users that either struggle with or are not comfortable with algorithm-only solutions.

To date, over 9 million users have been verified via ID.me’s alternative video chat pathway. Demographics that benefit most are lower-income populations, which coincides with the target beneficiaries of many government programs. ID.me has been able to double access rates for agencies

[13] Sherman, Justin. Testimony. “*Who is Selling Your Data?”* U.S. House of Representatives Energy and Commerce Subcommittee on Oversight and Investigations. April 19, 2023.
[14] Lima, Cristiano. The Washington Post. *Analysis | FTC consumer protection chief puts data brokers on notice*. September 21, 2023.
[15] Consumer Financial Protection Bureau. CFPB Explores Impact of Alternative Data on Credit Access for Consumers Who Are Credit Invisible. February 16, 2017.

when compared to algorithm-only solutions powered by credit bureaus and data brokers. In some instances, access rates were tripled for traditionally underserved demographics.[16]

Without ID.me and this alternative pathway, these users would have either been unable to access benefits or would have had to travel to a government agency to apply in-person. The act of visiting an agency and waiting in line to complete an application process in-person can be difficult for individuals with limited mobility, individuals who work outside the opening hours of agencies, or who struggle to find childcare. Giving users options means they can pick the pathway that works best for them.

Additionally, it is crucial that these verification pathways support multiple languages to cater to a diverse user base. This inclusivity ensures that linguistic barriers don't impede access. Adopting this multifaceted approach to identity verification ensures that no individual, irrespective of their circumstances or preferences, faces undue hindrances when accessing essential services and benefits. In essence, the bedrock of a secure and effective national benefit system lies in both robust identity verification practices and a streamlined approach to data retention. Only by synergizing these elements can we fortify our defenses against fraud while ensuring that genuine beneficiaries have unhindered access to the services and benefits to which they are entitled.

In testimony to the New Jersey State Assembly in 2022, the Commissioner of the New Jersey Department of Labor, Rob Asaro-Angelo, said, *"Let me be very clear about something: ID.me has increased equity in our system. Let me tell you why. Because folks in legacy systems, the way they were judged on if they were a high risk for fraud, was based on their banking, based on their credit history, based on if they owned a home, based on if they were transient workers or not. ID.me, all you need is your license or your passport or some other form of identification, that gets you through."* [17]

It is worth emphasizing, as pointed out by The Washington Post, that in 2020, less than half of the Americans aiming to set up an online account with the IRS were successful. Former IRS Commissioner Rettig aptly underscored this when he remarked on the IRS's previous system, stating it had a 40% authentication rate. This left 60% of users unable to access services digitally, compelling them to resort to in-person visits or phone calls. Working with ID.me, the IRS was able to get authentication rates well above 70%[18]. That rate has risen since Commissioner Rettig's testimony and continues to rise as we continue to add equity-enhancing features to our verification pathways. This underscores the widespread nature of this challenge and how solutions like ID.me are an absolute necessity in today's digital age.

Until 2022, a mere 23.9% of Puerto Rican taxpayers could successfully verify their identities online via the IRS Secure Access system.[19] This platform, dependent on data from credit bureaus and data brokers, left a significant portion of the population underserved. However, a paradigm shift occurred when ID.me came into the picture. By integrating with the IRS, ID.me facilitated a range of verification pathways, leading to a 3x increase in verification rates for users from Puerto Rico to 78.6% – a testament to their efficacy.

The Role of Biometrics and the Rising Threat of Generative AI-Driven Deepfakes

As digital fraud continues to evolve and threaten public benefits programs like UI, the integration of biometrics and advanced AI technologies is not just beneficial but essential. The rise of generative AI has

[16] Press Release. Puerto Rico Commissioner to Congress, Jenniffer González-Colon. IRS improves online identity verification for Puerto Ricans in response to Rep. Jenniffer González inquiry. June 8, 2023.
[17] Asaro-Angelo, Rob. New Jersey Assembly Budget Committee Hearing. May 04, 2022.
[18] Singletary, M. Washington Post. *Despite privacy concerns, ID.me nearly doubled the number of people able to create an IRS account.* Washington Post. February 25, 2022.
[19] Ibid.

enabled fraudsters to create highly convincing deepfakes, posing significant challenges to traditional fraud detection methods. Biometrics are an effective way to stop these attacks and should be used responsibly with human review and fallbacks.

Securing services via responsible use of biometrics

Deployment of biometrics for identity verification, including facial recognition and liveness detection, are included in NIST's digital identity guidelines, Special Publication 800-63-3. These technologies are effective at ensuring that users are genuinely who they claim to be, which is vital for preventing fraud in digital services, particularly for government benefits. A string of high-visibility data breaches, including 147 million consumers from Equifax and 22 million from the Office of Personnel Management, means that legacy methods of verification are no longer effective. With stolen personal information, fraudsters could now answer sensitive questions about an individual, rendering "knowledge-based verification" obsolete. NIST understood the need for new verification methods and included the requirement for "biometric or physical comparison" of the claimant to the strongest piece of evidence provided during the verification process.

At the same time, ID.me recognizes the sensitivities around the use of biometrics. This is why ID.me's use of biometrics is guided by design principles that should be adopted industry-wide and enforced via policy:

1. Use algorithms that have been demonstrated, in government testing by NIST and/or DHS, to (1) have industry-leading accuracy and (2) perform consistently across demographic groups
2. Back-stop them with human review when there is a non-positive outcome for the end user

This approach would be in line with the Biden Administration's Office of Science and Technology Policy's (OSTP) *Blueprint for an AI Bill of Rights,* which calls for "human alternatives, consideration, and fallbacks."[20] As far as we are aware, we are the only solution in the market that provides human review and fallbacks to users and the agencies they are trying to access.

Digital inclusion is under attack from fraudsters

ID.me's multiple verification pathways increase inclusiveness for underserved populations. However, the increasing sophistication of deepfakes is making it more difficult to secure these inclusive verification pathways. The U.S. Department of Homeland Security (DHS) has acknowledged the clear and present danger posed by synthetic content, which threatens various domains, including national security and financial sectors (Homeland Security, 2024). As an example of their effectiveness, a fraudster recently ran a deepfake scam in Hong Kong and was able to steal $25 million from a single company.[21]

Biometrics are an effective countermeasure to deepfakes and injection attacks. ID.me believes that biometrics will need to play an even bigger role in the protection of benefits in the future. Now is the right time to discuss how responsible use of biometrics, continuous human oversight, and threat research and monitoring, will enable the government to maintain its edge in the fight against digital fraud. Congress should work with the Executive Branch to avoid any form of blanket bans or restrictions on their use and advance guidelines for responsible deployment of biometrics, as outlined above.

[20] The White House. Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. October, 2022.
[21] Regan, H., & Hodge, N. CNN. Deepfake scam fools Hong Kong company into paying $25 million to fake CFO. February 4, 2024.

Reclaiming Fraudulent Payments: A Comprehensive Framework

The integrity of our national services and benefits programs hinges significantly on the robustness of our identity verification processes. Leveraging established best practices is essential in safeguarding these systems from fraudulent activities and ensuring that genuine beneficiaries have seamless access. My recommendations on strengthening these mechanisms is as follows:

1. **Adherence to NIST's Guidance on Identity Verification:** It's imperative for government agencies to align with the expertly crafted guidelines of the Department of Commerce's National Institute of Standards and Technology (NIST). These guidelines provide a clear roadmap for agencies to assess transactional risks and determine the appropriate identity assurance level (IAL) — ensuring that the level of identity verification rigor matches the potential risks associated with each service or benefit. By utilizing NIST's guidance, agencies can elevate their performance standards and secure their operations against malicious activities.

2. **Opting for NIST Identity Assurance Level 2 (IAL2) Policy**: From ID.me's experience in working alongside federal and state agencies, those that value strong fraud protections while distributing entitlement benefits typically gravitate towards the IAL2 policy. The rationale is grounded in the transaction's inherent risks and the attractiveness of these benefits to potential fraudsters. Some agencies opt for an initial verification process, while others grant users preliminary portal access with a lower assurance level, subsequently elevating the verification rigor to IAL2 during application initiation. Embracing IAL2 is demonstrably effective in thwarting fraudulent access, thereby ensuring that entitlement benefits reach their rightful beneficiaries.

3. **Establishing Uniformity in Data Retention for Prosecutorial Support:** Currently, the federal landscape is marked by a mosaic of data retention guidelines, with each agency marching to the beat of its own drum. This inconsistency often proves to be a bottleneck in prosecuting fraudulent activities. To overcome this, Congress should champion a standardized approach to data retention, ensuring that all agencies operate under a unified framework. An expert central authority, such as NIST or an alternative governing body, should be entrusted with the responsibility of crafting clear directives on the terms and tenure of data retention. With standardized guidelines, agencies will be better positioned to furnish evidence, bolstering the legal machinery's efforts to hold fraudsters accountable.

Integrating these state-of-the-art technological solutions has been instrumental in overcoming barriers to access that have long plagued the system.

Congressional Action and Future Initiatives

Legislative efforts like the *"Protecting Taxpayers and Victims of Unemployment Fraud Act"* are important to fully address the scope of issues exposed during the pandemic. This bill aims to recover fraudulent unemployment payments and improve the integrity of UI programs across states. Key provisions include incentivizing states to recover fraudulent funds by allowing them to retain 25% of recovered federal funds. This incentivizes state workforce agencies to invest in costly investigations and prosecutions that might otherwise be avoided due to lack of financial return.

Additionally, the bill proposes using the recovered funds to modernize state systems for verifying identity and income, and implement other program integrity activities. By retaining 5% of state UI overpayments recovered, states can further enhance their fraud prevention measures, ensuring UI claims are

cross-verified against the National Directory of New Hires and the State Information Data Exchange System.

Extending the statute of limitations for prosecuting fraud from 5 to 10 years, as recommended by the Pandemic Response Accountability Committee (PRAC), also provides a broader window to hold fraudsters accountable. The investment included in the FY2024 budget to enhance and preserve the PRAC's data analytics function, aligns with the goals of H.R. 1163 and underscores the broad bipartisan support for robust fraud prevention and recovery strategies.

It is evident that a comprehensive approach involving both state and federal efforts is essential to combat fraud effectively. It is also important to underscore that states have effectively demonstrated – when given the choice – they can efficiently leverage the competitive identity verification marketplace developed around the NIST guidelines as adopted by federal agencies under the Federal Information Security Modernization Act (FISMA) and subsequent guidance OMB M-19-17. Just as Congress added the identity verification requirement under Section 242 of the Continued Assistance Act to improve the integrity of the Pandemic Unemployment Assistance program, Congress should also consider further steps to add an identity verification requirement to traditional UI and subsequent UI programs.

Private sector identity verification solutions that conform to NIST standards, like ID.me, play a pivotal role in this ecosystem by providing the technological backbone needed to detect and prevent fraudulent activities, ensuring that benefits reach those who genuinely need them while protecting taxpayer dollars.

Conclusion

The digital landscape offers incredible opportunities for the future of effective public benefit service delivery but also significant challenges, particularly highlighted by the staggering losses due to fraud during the pandemic. Tackling these issues requires more than just government action. It calls for innovative private sector solutions working in harmony with governmental efforts to prevent fraud and enhance digital identity verification – and states being allowed the flexibility to choose from among the most secure, federally compliant options that best suits the needs of their residents.

Public networks systems are vulnerable, and the rapid disbursement of funds exposed these weaknesses. Accurate reporting on the extent of fraud varies, with estimates in the hundreds of billions of dollars. This discrepancy underscores the complexities in measuring and combating fraud effectively.

Members of Congress and decision-makers alike must understand that our national interest mandates support for initiatives that underscore technological integration and the harmonization of standards, particularly the NIST 800-63 digital identity guidelines. These are essential frameworks that ensure we stay ahead of those who seek to exploit the system. Jeremy Grant, the former advisor for the Obama-Biden administration's National Strategy for Trusted Identities in Cyberspace and now Director of the Better Identity Coalition, commented, *"IAL2 is not just a compliance requirement; in the world of remote identity proofing it is the line between a system that can fend off the bulk of identity theft attacks coming from organized criminals, and one that cannot.*"

Recovery and resilience extend beyond strict measures; they require fostering innovation where technology can thrive to recover stolen funds and prevent future losses. This effort must include continuous dialogue and cooperation between the private sector, tech partners, and government entities.

As we tackle these challenges, we owe it to the American taxpayer to implement forward-thinking strategies and robust infrastructures that ensure equity, security, and innovation. Together, let's aim for a secure future that benefits every American. Thank you for the opportunity to discuss these crucial issues.