Testimony of

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

"Action Through Innovation: Private Sector Solutions to Recouping Stolen Pandemic Loan Funds"

United States House of Representatives
Committee on Small Business
September 27, 2023

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 113 million users and more than 650 private sector partners, including 15 federal agencies and 36 state agencies. Of the 113 million users, over 48 million have active NIST credentials.

JT Taylor
Senior Director of Fraud
ID.me

Chairman Williams, Ranking Member Velázquez, and Members of the Small Business Committee: I am honored to be here today to present testimony about *Action Through Innovation: Private Sector Solutions to Recouping Stolen Pandemic Loan Funds*. My name is JT Taylor, and I serve as the Senior Director of Fraud at ID.me. Before this role, I dedicated a significant portion of my professional career to the U.S. Intelligence Community and the U.S. Military, serving in both as an intelligence operations officer. This experience imbued me with a deep understanding of intricate global security dynamics. Later, I served as a Special Agent with the United States Secret Service, where I led a series of pivotal domestic and international fraud and cybercrime investigations. My tenure in intelligence operations and my investigative endeavors have granted me a comprehensive and nuanced perspective on the challenges inherent to digital fraud and cyber threats. 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.

Historical Context

Before diving into the detailed response mechanisms to the COVID-19 pandemic, it is important to contrast it with a precedent: the 2009 Troubled Asset Relief Program (TARP). Instituted as an emergency measure in response to the financial crisis of 2008-2009, TARP was aimed at stabilizing the crumbling U.S. financial infrastructure, igniting economic growth, and warding off foreclosures that were otherwise preventable.

In October 2008, Congress initially authorized $700 billion for Troubled Asset Relief Program (TARP). However, this amount was subsequently revised and reduced to $475 billion by the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). In contrasting the federal government's response to the 2008 financial crisis with the economic fallout from the COVID-19 pandemic, it becomes evident that each crisis necessitated distinct approaches and oversight mechanisms.

TARP was a significant element of the government's response to the financial crisis of 2008. Recognizing the potential for fraud on such massive amounts of taxpayer dollars, Congress established the Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP). With a clear mandate to prevent and detect fraud, waste, and abuse related to the funds appropriated through the Emergency Economic Stabilization Act (EESA) and the Consolidated Appropriations Act of 2016, SIGTARP was positioned as a watchdog.

Armed with the authority to undertake investigations and conduct independent audits, this office was pivotal in ensuring that TARP funds were utilized efficiently, effectively, and in line with Congressional intent.

Fast forward to 2020, and the nation confronted a radically different crisis — a health pandemic with far-reaching economic repercussions. In response, Congress passed the Coronavirus Aid, Relief, and Economic Security (CARES) Act, a stimulus package dwarfing TARP in its magnitude, over four times as large with over $2 trillion earmarked to mitigate the pandemic's economic blow. Notably, the CARES Act did not come with an equivalent to SIGTARP, a singular dedicated oversight body. The absence of a specialized investigative agency specifically tailored for the CARES Act raised concerns about the potential for inefficiencies, fraud, or misuse of the allocated funds.

The differing oversight mechanisms between TARP and the CARES Act underscore the distinct challenges and priorities faced during each crisis. While TARP, conceived in the shadow of banking and financial malfeasance, emphasized stringent oversight to restore public trust, the CARES Act was a rapid response to an unpredictable and evolving pandemic, emphasizing quick dissemination of funds to ensure economic stability. Both responses were shaped by the unique exigencies of their respective moments, and it is evident that the CARES Act would have benefited from a more robust oversight structure akin to SIGTARP.

The CARES Act and Rampant Fraud

The economic challenges posed by the COVID-19 pandemic were unprecedented, demanding a swift and comprehensive response. Whereas TARP was a mechanism to address a financial crisis born out of risky banking practices and mortgage-backed securities, the situation in 2020 was a broad-based public health crisis that spilled over into every facet of the economy. Given the differences in context and scope, the U.S. government's response had to be tailored accordingly.

In March 2020, in reaction to the looming health and economic threats of COVID-19, Congress enacted and the President signed the CARES Act into law, architected with a primary goal: to deliver emergency assistance to the multitudes – both individuals and businesses – battered by the pandemic's repercussions.

In 2022, the Government Accountability Office (GAO) reported that the Federal government made improper payments totaling $247 billion, of which $200 billion were overpayments. This marks a distressing rise from $108 billion in 2012 to $247 billion in 2021.[1]

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

Multiple federal programs continue to hemorrhage taxpayer funds due to these improper payment rates. The COVID-19 pandemic further exacerbated the situation, laying bare significant vulnerabilities in our fraud prevention measures. The vital process of digital identity verification, meant to ensure users – especially those users 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 weak link, state-level benefits administrators stepped in, enforcing identity verification at diverse stages of the claims process. This insight is pivotal in understanding the backdrop against which my recommendations in this testimony are framed. In the absence of rigorous identity verification for digital government services, the door was left wide open for identity theft and fraudulent claims.

Early into the pandemic, ID.me established a Threat Intelligence Cell (TIC), which unearthed alarming fraudulent tutorials targeting the Small Business Administration (SBA), hosted on platforms like DocMerit and CourseHero. Such threat intelligence is crucial for agencies to fortify defenses, as evidenced by states like California, New York, and Florida, which – among several more – credit ID.me with helping stop approximately $273 billion in unemployment fraud.[2]

However, challenges persist. The latest GAO estimates suggest that unemployment insurance fraud during the pandemic could be between $100 billion and $135 billion.[3] From 2019 to 2020, the Federal Trade Commission saw a staggering 2,920% increase in identity theft reports associated with government document fraud.[4]

Revelations from the Fed ID Forum, backed by findings from both the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and the U.S. Department of Justice, indicate that $212 billion in suspicious 2021 transactions had ties to failures in identity verification.[5] Noteworthy comments from our national security officials equate the scale of this fraud to an economic assault on our nation.

The post-pandemic period still witnesses rampant fraud, challenging our prevention systems. Despite the proven efficacy of the Department of Commerce's National Institute of Standards

---

[2]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.

[3] Government Accountability Office (GAO) Report: *More Fraud Has Been Found in Federal COVID Funding—How Much Was Lost Under Unemployment Insurance Programs*. September 13, 2023.

[4]*Federal Trade Commission. 2020 Consumer Sentinel Network Data Book, last accessed, September 24, 2023.*

[5]Martin, Zach. Center for Cybersecurity Policy. *FinCEN: $212 billion in likely financial crimes linked to identity verification breakdowns*. September 13, 2023.

and Technology (NIST) identity assurance standards during the pandemic, some jurisdictions, like Colorado, opted for alternative solutions, resulting in a surge of fraud and innumerable citizens denied their rightful benefits. States such as Ohio and Connecticut are still grappling with fraudulent onslaughts, illustrating the widespread and ongoing nature of this issue.[6][7] Our nation faces a persistent and multifaceted threat from fraud, and concerted, coordinated efforts are required to address and rectify these vulnerabilities.

The Paycheck Protection Program (PPP)

A noteworthy initiative within the CARES Act was the inception of the Paycheck Protection Program (PPP) in April 2020. Administered by the SBA, the PPP became a lifeline for a spectrum of entities – small businesses, nonprofits, and individuals. The program presented fully guaranteed loans, which were forgivable under specific conditions, enabling businesses to manage payroll costs, including benefits, as well as rent, utilities, and mortgage interest expenses.

Complementing the PPP, the SBA also championed the COVID-19 Economic Injury Disaster Loan (EIDL) program and a related EIDL grant initiative. These were devised to offer a financial cushion to businesses and other organizations grappling with the economic tremors of the pandemic. The EIDL program, in particular, facilitated low-interest, fixed-rate, long-term loans, giving borrowers the crucial working capital to cover routine and essential operational costs.

For perspective, the SBA was entrusted to oversee an unparalleled volume of funds through both the COVID-19 EIDL program and PPP. The deployment was impressive: more than $400 billion was disbursed as COVID-19 EIDL funds, and the PPP scheme saw nearly $800 billion channeled through third-party lending partners.[8]

At the onset of the pandemic, it was evident that the SBA would confront a complex situation: delivering swift relief to Americans in dire need, while also establishing necessary safeguards against the potential for rampant fraud. A predominant concern emerged when the SBA prioritized the rapid distribution of funds to eligible small businesses, potentially overlooking vital internal controls that would reduce the likelihood of fraudulent activity. Such controls include verification processes to ensure that businesses seeking aid genuinely existed before the pandemic and were genuinely impacted by the subsequent economic challenges.

The SBA Office of Inspector General (SBA-OIG), recognizing these challenges, proactively issued two reports even before the first PPP loan was disbursed. In these reports, the emphasis was placed on the necessity of solid, upfront program controls designed to diminish fraud risks.

---

[6] Allen, Jaclyn. Denver7. *Surge in Colorado unemployment fraud affects legitimate claims.* July 25, 2023.

[7] Polansky, Rob. Eyewitness News2. *Labor department suspects 75 percent of unemployment claims are fraudulent* July 21, 2023.

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

Given the lessons from previous disasters, it was clear that any vulnerabilities in oversight or process, when applied to massive undertakings like the COVID-19 EIDL program and PPP, could lead to significant challenges and potential misuse of funds.[9]

From my vantage point as a then Senior Special Agent for the U.S. Secret Service, when the SBA sought to expedite their disaster loan programs to offer immediate relief, they inherently risked heightening their vulnerability to fraudulent activities and financial losses. The unprecedented surge in loan application volume, fueled by the pandemic, naturally strained their existing oversight mechanisms.

Recognizing this, it became crucial to equip the SBA with insights from previous audits and inspections, especially those that highlighted risks associated with swiftly processing large volumes of loans. To maintain the integrity of these disaster relief programs and reduce the possibility of financial setbacks, it was paramount that the SBA ensured loans were only granted to genuine, eligible applicants. Moreover, the agency needed skilled and adequately trained staff to manage the sheer volume of loans and the urgency surrounding their disbursement.

While the PPP's vast scale and ambition were evident, the SBA-OIG recommended several pivotal measures to curb potential financial losses as loans were rapidly rolled out to qualifying small businesses. This involved instituting strict controls during the loan sanctioning process to rigorously identify participants. The SBA's significant role in navigating the country through the pandemic was unparalleled. Yet, the OIG's anticipatory white paper reports did presage some of the internal challenges the SBA would face in administering the PPP and COVID-19 EIDL initiatives. The SBA managed to facilitate a volume of lending equivalent to 14 years, all within a two-week span. But as the total value of pandemic relief efforts surged past the trillion-dollar mark, it became evident that the SBA preferred a process that was primarily necessitated towards a speedy allocation of funds, inadvertently amplifying risks to taxpayers.

Additionally, some lenders exacerbated fraud vulnerabilities by valuing speed and potential revenue over a meticulous examination of applicant qualifications for governmental support. As an illustration, one particular lender ramped up its loan processing from a mere 200 loans annually to nearly half a million within the pandemic's span, without significantly boosting its workforce or enhancing security protocols.[10] This pursuit of greater profit margins compromised their primary responsibilities, leading to an uptick in identity and eligibility fraud within their loan portfolio. This not only affected taxpayers but also undermined the primary economic objectives of the PPP.

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

During the SBA's efforts to respond to the pandemic, the OIG underscored several crucial recommendations to bolster the agency's safeguards against potential fraud, especially concerning the COVID-19 EIDL program and the PPP. The main takeaways from those suggestions are worth highlighting:[11]

- Confirm that loan values don't surpass the stipulated amount per employee.
- Validate that the business was operational before the specified cutoff date.
- They proposed a joint effort with the U.S. Department of the Treasury to create a technical mechanism. This would leverage Treasury's 'Do Not Pay' portal to screen PPP loan applicants, thereby avoiding unwarranted payments and securing federal funds.
- Modify the PPP application to gather borrowers' demographic details.
- Ensuring loans are credited solely to genuine bank accounts of eligible borrowers.
- Prohibiting post-approval alterations to loan application data unless reevaluated by a human reviewer.
- Obtain the applicant's photo ID for identity verification.
- Authenticate the legitimacy of the business using tax records, registration documents, or other relevant means.
- Establish human interactions for applicants with multiple submissions using the same identifiers, like IP or email addresses, to ascertain their authenticity.
- Craft a system that rapidly spots potential risk indicators and necessitates comprehensive mitigation before loan approval.
- Halting any duplicate applications that share identical Employer Identification Numbers (EIN) or Social Security Numbers (SSN).
- Setting up mechanisms that can instantly lock applications with identifiers (like EINs, SSNs, or IP addresses) previously tied to fraudulent activity, ensuring no further malicious submissions.
- Confirming EINs were established prior to the qualifying date for eligibility.

From an outsider's perspective, these recommendations reflect a comprehensive and meticulous approach to ensuring that the SBA's disbursement of critical pandemic-related aid adhered to the highest standards of integrity and accuracy. According to the investigations and data analysis by the SBA-OIG, there appears to be potential fraud exceeding $200 billion associated with the COVID-19 EIDLs and PPP loans.[12]

By harnessing advanced data analytics, past OIG reports, and rigorous investigative techniques, the SBA OIG found that of the funds disbursed, about 17% were potentially fraudulent,

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

comprising over $136 billion from the COVID-19 EIDLs and $64 billion attributed to the PPP loans.[13]

When viewed from a broader perspective, this lapse can be traced back to the SBA's inadequate internal controls in the verification, approval, and disbursement processes. This lack of oversight left the door open for malicious actors, depriving genuine businesses in dire need due to the pandemic's impact from accessing the intended financial support.

To recover a portion of these illicitly acquired funds, investigators must undertake meticulous casework constructed around the digital evidence these wrongdoers inadvertently left behind. These digital breadcrumbs, or "fingerprints," are pivotal in establishing the "Probable Cause to Search." The legal premise of this concept can be elucidated as follows: For the courts to issue a search warrant, they weigh the entirety of the available information to determine whether there's a reasonable likelihood that illegal items, pertinent evidence, or individuals connected to the crime can be located in a specific location.

In observing the actions of the SBA during this crucial period of economic relief, it became clear that there were vulnerabilities in their fraud control mechanisms. SBA-OIG has worked diligently to identify these vulnerabilities and brought several key fraud indicators to light.

As an impartial observer, I would like to share these observations that may guide future investigations:

IP Addresses: SBA-OIG discovered instances where loan applications, under the COVID-19 EIDL and PPP umbrella, were reportedly submitted either from foreign countries or from IP addresses that matched other suspicious applications.

Employer Identification Numbers (EIN): The SBA-OIG found irregularities in the usage of EINs. Some borrowers' EINs either coincided with other PPP loans or were improperly structured, leading to doubts about their authenticity.

Business Establishment Dates: There were cases identified by the SBA-OIG where borrowers claimed their businesses were established after the prescribed cutoff date, suggesting these entities were not eligible for assistance in the first place.

Phone Number Discrepancies: Upon close inspection, the SBA-OIG noted that certain phone numbers were repetitively used across multiple PPP and EIDL applications.

[13] U.S. Small Business Administration, Office of Inspector General. Report. *COVID-19 Pandemic EIDL and PPP Loan Fraud Landscape*. June 27, 2023.

Physical Address Irregularities: Similarly, the SBA-OIG flagged numerous instances where applicants used identical physical addresses across a multitude of applications.

Email Address Concerns: The SBA-OIG also highlighted concerns with the use of temporary email domains by applicants, which typically become obsolete after a short span. Furthermore, the crafty use of symbols like dashes and plus signs in email addresses indicated a probable attempt to bypass system checks by managing multiple accounts from a single email.

In reflecting upon the aftermath of the pandemic and the governmental response, one can't help but draw parallels between the vulnerabilities identified in the SBA's loan programs and the challenges faced by the Department of Labor (DOL) and state workforce agencies. As we begin to analyze and comprehend the full spectrum of issues, it's evident that there are shared pain points and lessons to be gleaned.

Interlinked Vulnerabilities: SBA and DOL

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, found themselves turning 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.[14]

It is worth noting that just a few years ago, certain states reported notable budget surpluses.[15] The failure to utilize these surpluses towards offsetting unemployment debts has resulted in mounting dissatisfaction among business owners. They now confront the financial repercussions of a crisis not of their making, compounded by the fact that many had to shutter operations due to pandemic mandates.

[14] Ohanian, Lee. Hoover Institution. (n.d.). *California defaults on $18.5 billion debt, leaving state businesses holding the bag*. April 11, 2023.
[15] Theal, J., & Fleming, J. The Pew Charitable Trusts. *Budget Surpluses Push States' Financial Reserves to All-Time Highs* May 10, 2022.

Highlighting this situation emphasizes the close-knit relationship between the unemployment benefits system and the health of small businesses. Fraud in unemployment programs doesn't just drain crucial funds; it indirectly threatens the very viability of small businesses, often considered the backbone of our communities. It is essential for policymakers to understand and address this intertwined challenge as Congress deliberates the path ahead.

Both the SBA and the DOL, along with state workforce agencies, encountered an unprecedented surge in the demand for financial relief. With programs like the Pandemic Unemployment Assistance (PUA), Pandemic Emergency Unemployment Compensation (PEUC), and Federal Emergency Unemployment Compensation (FEUC), the disbursement of well over a trillion dollars was no minor feat. While the urgency of the situation necessitated swift action, it inevitably brought to light areas of potential fraud and misuse.

Some common indicators of fraud that emerged in both contexts include questionable IP addresses, duplicative physical and email addresses, and the misuse of identification numbers. Additionally, the sheer volume and velocity of claims and applications made it challenging for these institutions to establish rigorous checks and balances in real-time.

In our eagerness to move beyond the pandemic's hardships, we must be cautious not to overlook the insights these experiences have afforded us. As stewards of public funds and trust, both the SBA and the DOL, together with state entities, have a responsibility to refine their processes, drawing from these lessons. As we prepare for future emergencies, we must prioritize developing more resilient, secure, and efficient systems to ensure that assistance reaches those in need while minimizing the scope for misuse.

Reflecting on the challenges and vulnerabilities of our financial systems, especially in the wake of the pandemic's economic relief programs, it becomes evident that we need robust solutions. Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes, Elizabeth Rosenberg, aptly highlighted this in her remarks on January 24, 2022.[16] She observed, *"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."

[16] Elizabeth Rosenberg, Assistant Secretary for Terrorist Financing and Financial Crimes, U.S. Treasury. Remarks at Better Identity Coalition. February 1, 2022.

During the tumultuous period 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, 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.[17] The successful application of NIST standards and robust fraud controls by ID.me played a pivotal role in fortifying security. The SBA's decision not to adopt NIST highlights the potential risks and pitfalls agencies expose themselves to when they don't adhere to the guidelines set forth in OMB M-19-17. It's crucial to underscore the implications of not following these established standards.

Between September 2021 and January 2022, ID.me's Threat Intelligence Cell (TIC) delved deep into the recesses of the dark web to study the prominent players, techniques, and tactics, techniques, and procedures (TTPs) that had targeted the SBA and EIDL loan systems. Their findings illuminated a concerning landscape:

Tutorials Market: The dark web was rife with detailed tutorials on executing fraudulent SBA and EIDL loan applications. These guides meticulously instructed potential fraudsters on the art of using stolen identity data without leaving digital footprints, ensuring a near-seamless theft.

Identity Hunt: A sizeable chunk of the dark web's activity around SBA loans revolved around procuring personal identifying information. The intent was clear: to impersonate genuine businesses and siphon off funds meant for them.

Collaborative Fraud: Many on the dark web sought accomplices for SBA-related fraud. This collaboration hinted at the possibility of multiple players orchestrating large-scale frauds rather than isolated incidents.

Infamous Actors: The dark web had its stars in the world of SBA fraud. Names like Kpoyaga, Krabon Mega, and A stood out, especially as they operated the well-frequented Telegram channel, Kpoyagahack, where they regularly shared insights on exploiting the SBA system. Another noteworthy actor, Ranhacker, had been credited with creating SBA fraud guides that had been spotted on platforms like DocMerit and CourseHero.

---

[17] 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.

As an observer, it was evident that the dark web had fostered a thriving ecosystem around SBA and EIDL loan fraud, with its actors evolving and adapting swiftly to exploit vulnerabilities. ID.me's TIC has been unrelenting in its dark web surveillance, consistently keeping tabs on nefarious activities targeting the SBA. In its persistent efforts, the cell has recently unearthed dark web posts that elucidate strategies and tactics for defrauding the SBA. The existence of such recent material is indicative of the ongoing threats and underscores the necessity for continuous vigilance and adaptive countermeasures.

A critical oversight by entities like the SBA mirrored the challenges faced by the DOL: they confused identity validation with identity verification. While the former merely ascertains that a combination of a Name, Date of Birth, and Social Security Number is genuine and accurate, the latter dives deeper, ensuring that the individual claiming an identity is indeed the rightful owner of that identity.

The vulnerabilities in relying on identity validation have been brutally exposed due to the plethora of data breaches. 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, malefactors found it easy to deceitfully claim pandemic assistance 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.[18]

The ripples of such activities have a profound human cost. As spotlighted by ProPublica, consider the ordeal of Philip Payton, a violinist for Disney's Frozen musical. Left jobless due to the pandemic, his identity was misused by a criminal to file an unemployment claim in Texas. This fraudulent action triggered a suspension of his genuine unemployment benefits in New York, given the restriction of claiming benefits in one state at a time for specific programs.[19]

The crux of the issue was the inability of these states to distinguish genuine claimants like Mr. Payton from malevolent actors due to inadequate identity verification measures. Tragically, he was left without unemployment benefits from September 2020 to April 2021. His story isn't an isolated incident but echoes the experiences of countless other Americans who suffered similarly.

[18] Penzenstadler, Nick. USA Today. *How scammers siphoned $36B in fraudulent unemployment payments from US. December 30, 2020.*
[19] Hall, Blake. Forbes Technology Council. Council Post. *How Fraud Reduces Access To Benefits*. February 16, 2023.

The widespread and accelerated adoption of the IAL2/AAL2 standard could have served as a robust barrier against the rampant fraud witnessed 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 could pave the way for enhanced interoperability across federal and state agencies. This, in turn, would lead to a more streamlined and positive experience for consumers.

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

The thriving realm of data brokers has emerged as a potential pitfall in the seamless execution of various state and federal economic relief 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.[20] 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 via the SBA.

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 Experian – one of the nation's major credit bureaus.[21] Such instances expose the deep-seated vulnerabilities of data brokers and their consequential impact.

---

[20] Krebs, B. KrebsOnSecurity. *Hacked Data Broker Accounts Fueled Phony COVID Loans, Unemployment Claims. Krebs on Security. August 21, 2020.*

[21] Ibid.

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.

Fraudsters typically cash out through money mules, cryptocurrency, prepaid cards, or online-only banks. These instruments allowed for substantial transaction amounts, making them especially attractive for such fraudulent activities.

In light of the revelations brought forth in the speech by the FTC's consumer protection chief, Samuel Levine, it's essential to reassess the expanding footprint of data brokers in the modern digital age. The exponential rise of the data brokerage industry, which amassed a valuation of $240 billion in 2021 and is on track to nearly double by the end of the decade, is not just an economic marvel but poses tangible threats to individual privacy.[22]

Consider this: Data brokers, as Mr. Levine duly noted, wield the power to build intricate profiles about Americans, down to their most private preferences and habits. This power, unchecked and unchallenged, veers dangerously close to infringing upon an individual's right to privacy.[23] In a society where information can be weaponized, do we truly want such intricate details of our lives readily available, often without our explicit consent?

Furthermore, while the industry may justify its practices under the guise of providing customized experiences or streamlining business operations, the undeniable truth remains that individuals rarely have a say in how their data is collected, stored, and shared. Mr. Levine's observations on the industry's "fever" in gathering and selling data are poignant. It's an uncontrolled race where the finish line is unknown, and the implications for individual privacy are extensive.

In a world of increasing transparency, shouldn't we hold data brokers to a similar standard? Levine's call for greater clarity in how companies interact with consumer data is not just sound advice but a foundational principle for safeguarding democratic values. Transparency is not just about business ethics but about protecting the very fabric of our society.

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."[24] The

---

[22] Lima, Cristiano. The Washington Post. *Analysis | FTC consumer protection chief puts data brokers on notice*. The Washington Post. September 21, 2023.
[23] Ibid.
[24] Sherman, Justin. Testimony. "*Who is Selling Your Data?"* U.S. House of Representatives Energy and Commerce Subcommittee on Oversight and Investigations.

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.[25] 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.

Enhancing SBA's Digital Security & Reclaiming Fraudulent Payments: A Comprehensive Framework

In this testimony, key recommendations are presented to strengthen the Small Business Administration's security framework and enhance its ability to recoup payments that have been mistakenly or fraudulently distributed. Insights from other federal agencies serve as valuable precedents for these suggestions.

1. **Adoption of a Robust Digital Identity Verification System:** Various federal institutions, encompassing the likes of IRS, DOD, and SSA, have successfully integrated digital identity solutions, like ID.me, into their operational framework. These systems, anchored in the guidelines set forth by NIST, equip these agencies with formidable security features. The SBA should likewise integrate such solutions.

2. **Identity Proofing:** It is crucial to ensure that users of public portals are thoroughly verified in alignment with the standards of NIST SP 800-63-3. This guarantees that individuals accessing federal benefits are genuinely who they purport to be.

3. **Empowering User Consent and Control:** Congress should enshrine in legislation the principle that users have the right to granular control over their data. Specifically:

    a. **Granular Consent Mechanisms:** Agencies and businesses should deploy systems that allow users to grant or deny consent for individual uses of their data. This level of specificity empowers users, ensuring they aren't faced with an all-or-nothing choice. For example, users could allow their data to be used for service enhancements but deny its use for commercial advertising.

[25] Lima, Cristiano. The Washington Post. *Analysis* | *FTC consumer protection chief puts data brokers on notice*. September 21, 2023.

b. **Transparency in Commercial Use:** It's paramount that users are made explicitly aware of any potential commercial (revenue-generating) uses of their data. Clear, concise, and easily accessible disclosures should be provided, outlining exactly how data will be used, by whom, and for what purpose.
c. **Dynamic Control Mechanisms:** Beyond initial consent, users should have the continuous ability to modify their preferences, granting or revoking permissions as they see fit. This dynamic control ensures that consent remains a living choice, adaptable to changing circumstances or user perspectives.
d. **Audit Trails & Accountability:** To bolster trust and compliance, there should be secure audit trails for consent actions. This will serve as a record of what permissions were given, when, and under what conditions. Such trails not only protect users but also provide organizations with a clear record, minimizing potential disputes.
e. **Protection from Coercion:** It's crucial to ensure that users are not penalized or deprived of essential services for refusing to grant consent for commercial use of their data. Consent should be freely given, without fear of negative repercussions.

4. **Prioritizing Security and Data Protection:** The chosen identity solutions should adhere to the standards of FedRAMP Moderate authorization. This commitment ensures the confidentiality, integrity, and overall availability of sensitive data.

5. **Flexibility in Login Options, Maintaining Security:** It is my belief that while fortifying digital defenses, there shouldn't be a compromise on user choice and accessibility. Hence, Congress should consider empowering federal agencies to furnish multiple login alternatives for users. This flexibility should, however, remain within the confines of government-set guidelines. The outcomes of this dual approach not only maximizes access for marginalized groups but also drives down operational expenditures for agencies.

6. **Unified Federal Framework:** Drawing inspiration from countries like Estonia, Sweden, and Norway, where government-issued credentials grant access to various public services, the U.S. should enforce a more harmonized approach. Specifically, the Office of Management and Budget (OMB) Memorandum-19-17 (M-19-17) advocates for a system wherein Americans can choose from either federally or commercially provided shared services, such as ID.me, for identity verification. This model, analogous to the function of digital wallets like PayPal, would facilitate user access while maintaining rigorous security standards.

7. **Reinforced Security Measures:** Evidence suggests that aligning with NIST's Identity Assurance Level 2 (IAL2) standards significantly amplifies the protective measures

against fraudulent activities. For instance, ID.me's adherence to these standards helped save an astounding $273 billion in unemployment funds. Contrarily, deviations from these standards have been met with consequential fraudulent activities.

8. **Strict Adherence and Oversight:** To ensure robust security, the application of the NIST 800-63-3 framework is paramount. This would allow institutions to leverage top-tier cybersecurity knowledge, adapt their protocols as per the risk context, and foster innovation in fraud prevention. A vibrant marketplace already offers Software as a service (SaaS) solutions in line with these standards, ensuring financial institutions remain agile in a dynamically challenging environment. To bolster this, an independent accreditation mechanism should be put in place, steered by an autonomous governance body, distinct from agencies that develop these solutions. This body would ensure conformity, frame performance metrics, and certify providers.

9. **Broadened Data Validation Access:** The Social Security Administration currently offers an electronic Consent Based Social Security Number Verification (eCBSV) tool. This tool, however, is solely accessible to financial institutions. Expanding access to this tool beyond these institutions, especially to approved Credential Service Providers (CSP), would address equity concerns and ensure a wider demographic enjoys unhindered access.

10. **Standardized User Interface Across Portals:** It's pivotal that agencies adopt a uniform user interface for their online platforms, allowing users the liberty to select their identity verification provider and the mode of this verification. Initiated with platforms like Login.gov and ID.me, this would be open to other service providers that adhere to the NIST guidelines and have acquired independent accreditation. Such a standardized interface ensures consumers can elect the most suitable provider for them, reaping the benefits of a competitive landscape.

    To ensure equitable and comprehensive access to public services and benefits, it's imperative that agencies implement versatile identity verification methods, catering to diverse user needs and preferences. These recommendations, derived from the best practices of entities like ID.me, are essential for reaching the entirety of our population, especially the underserved segments.

11. **Flexible Identity Verification Mechanisms:** Agencies must embrace solutions that provide users multiple avenues for identity verification, ensuring no undue burden is placed on the agency or the user. The versatility of these methods ensures that every individual can select a mode that aligns with their comfort and accessibility levels.

a. **Online Self-Service Verification:** This approach allows individuals to independently validate their identity online, typically completing the process in a short span. It's worth noting that a significant majority, approximately 85-90% of users at federal agencies, prefer and utilize this method for its efficiency.

b. **Remote-Assisted Verification via Video Chat:** For individuals whose details might be outdated, missing, or incorrect in credit or public databases, a remote-assisted verification method becomes invaluable.
Here, users can authenticate their identities by interacting with a trained professional through a video call. This method is particularly advantageous for demographics like students with minimal or no credit footprints, recent migrants, or those who've undergone a name change. Evidence from ID.me indicates that this method has successfully verified millions who might have otherwise faced verification barriers.

c. **In-Person Verification Points:** Lastly, a conventional, face-to-face verification method remains pivotal. This allows individuals to confirm their identity at designated physical outlets. With over 680 such retail locations across the nation, it ensures those uncomfortable or unfamiliar with digital means have an accessible alternative.

The integrity of our national services and benefits 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. Here are my reflections and recommendations on strengthening these mechanisms:

12. **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.

13. **Opting for NIST Identity Assurance Level 2 (IAL2) Policy**: From ID.me's experience in working alongside federal and state agencies, those that distribute 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.

14. **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.

Furthermore, it's crucial that each of these verification pathways cater to a multicultural user base by supporting multiple languages. 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 fraudulent elements while ensuring that genuine beneficiaries have unhindered access to the services and benefits they are entitled to.

During my examination of the ever-growing digital landscape, ID.me's NIST 800-63-3 IAL2/AAL2 conformant solution has emerged as a powerful tool to both deter fraud and ensure proper identity verification, in ways that simultaneously advance the dual goals of equity and access. This is particularly pertinent in light of the challenges that various populations face, such as communities in Puerto Rico, when trying to access critical online services.

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%[26]. This underscores the widespread nature of this challenge and how solutions like ID.me are an absolute necessity in today's digital age.

[26] 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.

Puerto Rico's Resident Commissioner to Congress, Jenniffer González-Colón shed light on this concern when gathering insights about the actions the Internal Revenue Service (IRS) was undertaking to enhance its services and accessibility for Puerto Ricans. The encouraging news that followed her inquiry highlighted how new technologies, like those implemented by ID.me, play a pivotal role in bridging these gaps.[27]

Until 2022, a mere 23.9% of Puerto Rican taxpayers could successfully verify their identities online via the IRS Secure Access system.[28] 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 staggering rise in Puerto Rican verification success rates to 78.6% – a testament to their efficacy.

This groundbreaking transformation comes at a time when Congress, in a bipartisan effort, scrutinizes the role and practices of data brokers and credit bureaus, especially in the realms of data collection, licensing, selling, and utilization. The evidence is clear: data brokers often falter when it comes to verifying individuals who've experienced recent relocations, name changes, or those who might have minimal credit records. Such shortcomings stress the importance of adopting more innovative solutions from the private sector.

The integration of these state-of-the-art technological solutions has been instrumental in overcoming barriers to access that have long plagued the system. Residents of Puerto Rico deserve seamless authentication, ensuring that they can tap into the critical federal benefits and programs for which they are eligible.

Conclusion

The vast expanse of the digital frontier presents both unprecedented opportunities and challenges. One of the most glaring issues arising from the rapid disbursement of unemployment and small business relief during the pandemic was the loss of hundreds of billions of dollars to fraudulent activities. The sheer magnitude of this loss underscores the vulnerabilities in our current systems and the urgent need for remedial action.

I look forward to discussing the fact that combating these issues cannot solely be a governmental endeavor. There's a palpable need for innovative solutions from the private sector, working symbiotically with governmental efforts, to bring about real, effective change, thwart bad actors, and refine the digital identity experience. The theft of pandemic loan funds showcases the

[27] Congresswoman Jenniffer González-Colón. Press Release. *IRS improves online identity verification for Puerto Ricans in response to rep. Jenniffer González inquiry.* June 8, 2023.
[28] Ibid.

evolving nature of fraudulent activities, and our countermeasures must be equally adaptive, leveraging technology to its full potential.

To Members of Congress and decision-makers alike, the road ahead is clear. Our national interest mandates support for initiatives that underscore technological integration and the harmonization of standards, particularly the NIST 800-63 guidelines. These aren't just bureaucratic checkboxes but essential frameworks that ensure we're always a step 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."[29]

However, the path to recovery and resilience is more than just about stringent measures. It's about fostering an ecosystem of innovation – where our technological capabilities can truly shine in recovering stolen funds and preventing further losses.

Such innovation necessitates continued dialogue and, more importantly, cooperation between the private sector, technological partners, and the government. The synergy from this triad can maximize the efficacy of our recovery efforts and create a robust system, resilient to the multifaceted challenges of the modern era.

In reflection, the trials we've grappled with illuminate the pivotal juncture we stand at today. The American taxpayer, the backbone of our nation, rightfully deserves more. Fortified by collective resilience, forward-thinking strategies, and an unwavering resolve, we're not merely aiming to regain lost ground. We're setting our sights on a future where we craft infrastructures that epitomize security, innovation, and consumer choice. Together, let's chart this ambitious course, driven by our shared aspirations for a more secure tomorrow and our duty to every American taxpayer.

[29] Grant, Jeremy. NextGov/FCW. *Why it's time for a pivot on digital identity*. March 14, 2023.