COVINGTON

BEIJING BRUSSELS DUBAI FRANKFURT JOHANNESBURG
LONDON LOS ANGELES NEW YORK PALO ALTO
SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

Robert K. Kelner

Covington & Burling LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956
T +1 202 662 5503
rkelner@cov.com

April 28, 2022

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
U.S. House of Representatives
Washington, DC 20515

The Honorable James E. Clyburn
Chairman
Select Subcommittee on the Coronavirus Crisis
U.S. House of Representatives
Washington, DC 20515

Dear Chairwoman Maloney and Chairman Clyburn:

On behalf of our client ID.me, Inc. ("ID.me"), this letter responds to your April 14, 2022 letter to ID.me. ID.me appreciates the opportunity to provide information regarding the company's innovative identity-verification service, as well as the company's proactive efforts to expand access to critical government services during the COVID-19 pandemic, its practices with respect to compliance with federal identity-verification standards, and its policies regarding the retention of information provided by users during the identity-verification process. We also hope that this letter will serve to correct what we believe to be inaccurate or incomplete information that has been reported in the media.

As discussed with your staff, this is an initial response, and we anticipate providing additional documents and information on a rolling basis. In particular, this letter includes ID.me's responses to Requests 1, 2, 3, and 4, as well as Questions 1, 3, and 5, included in your April 14 letter. The company's review of these matters is ongoing, and the information below is provided to the best of our current understanding.

Introduction

With grant funding from the National Institute of Standards and Technology ("NIST"), ID.me developed its digital identity services under the principles of the Obama/Biden National Strategy for Trusted Identities in Cyberspace. The grant funding supported the company's efforts to build a privacy-enhancing, secure, and interoperable identity-verification service to put users in control of their data while adhering to government standards.

ID.me originally focused on assisting American veterans to securely prove their veteran status online. Veterans could do this once and then reuse that credential to access military discounts and other benefits. The company has evolved to develop innovative services that increase secure access to services via digital channels, improve customer experience through portable credentials, and offer a consumer-centric model for digital identity. ID.me puts consumers in control of their personal information by requiring consumers' consent to share their data with what NIST calls "relying parties" within government and the private sector. No personal information is transmitted without this consent, and ID.me shares only the personal information required by its partners to complete the transaction initiated by the user.

From its origins serving members of the military community, the company expanded to provide identity-verification services to a diverse array of public and private partners, enabling online access to vital services and benefits for students, teachers, nurses, first responders, and government employees. Today, the ID.me secure digital identity network supports 86 million users with over 145,000 individuals joining daily, as well as partnerships with 31 states, multiple federal agencies, and over 500 name-brand private sector companies.

Ultimately, ID.me's mission is to make the world a more trusted place by delivering the highest level of security with the least amount of friction at the lowest possible cost. To that end, the company's digital identity network improves the user experience by eliminating the need for users to verify at each new organization from which they want to access services. A user verifies their identity once, creating a portable digital identity credential, and then can safely and securely bring proof of their identity wherever the credential is accepted. The user controls when and with whom their data is shared.

Legacy Identification-Verification Methods

To understand ID.me's online identification verification technology, it is important to bear in mind how users have traditionally verified their identities when seeking government benefits or other services offline. Historically, when seeking access to benefits or services, people were generally required to travel to an office or other location and present a physical document—for example, a driver's license, military identification card, or student identification card—to a human agent responsible for comparing the image on the document to the appearance of the person standing before them.

This historical model presented a number of inherent concerns. Most obviously, this method of identity verification required those seeking services to travel in-person to particular locations to offer proof of their identities. Visits to physical locations to verify identity require travel time, are limited by office hours, and can be more difficult for individuals with mobility issues. Likewise, reliance on in-person verification proved particularly untenable in the wake of the COVID-19 pandemic. Indeed, at a time when the demand for government services was at its height, many government offices and other physical locations at which people could verify their identities and demonstrate their eligibility for services were either operating on limited schedules or closed entirely.

Moreover, even where online verification options were available, traditional identity-verification options were hampered by reliability and security concerns, raising the risks both of potential fraud and of unequal access to vital services. For example, many legacy methods of identity verification, such as so-called knowledge-based verification (*i.e.*, proving identity through questions and answers), rely on information collected by credit rating agencies and other financial institutions.

Unfortunately, our recent experience fighting unemployment insurance fraud has shown how readily available such information is to malicious actors, presenting a significant risk of identity theft and fraud. At the same time, the types of credit history information relied upon by legacy identity-verification methods is simply unavailable for tens of millions of Americans, with

this barrier to access falling disproportionately on low-income and minority populations. For example, in 2016, the Consumer Financial Protection Bureau estimated that 26 million Americans do not have a credit history with one of the nationwide credit reporting companies, with Black and Hispanic Americans more likely to be "credit invisible."[1] An additional 19 million Americans have thin or otherwise dated credit history that can limit their abilities to verify their identities through legacy verification methods.

Recognizing the inherent limitations of legacy identity-verification methods, and in the wake of a series of data breaches that rendered knowledge-based verification ineffective, NIST published new federal digital identity guidelines in 2017. These guidelines call for the use of biometric or physical comparison of an individual's appearance to photographic evidence of a person's identity.[2] For high-risk transactions, NIST recommends adoption of their Identity Assurance Level 2 ("IAL2") and Authenticator Assurance Level ("AAL2") standards. Nonetheless, many government agencies continue to rely on legacy, credit-based identity verification methods.

ID.me's Identity-Verification Service

Consistent with NIST's IAL2 and AAL2 guidelines, ID.me's identity-verification technology allows users to safely and securely verify their identity. The two primary pathways to verification described below are defined by NIST. ID.me's service offerings adhere to the guidelines set forth by NIST for each of these pathways. In all instances, ID.me is committed to increasing the number of users with access to digital channels and does so by offering users a variety of pathways through which they may verify their identities and obtain services or benefits from ID.me's partners.

Unsupervised Remote: In order to adhere to NIST guidelines for Unsupervised Remote identity proofing at IAL2, ID.me must work with the user to collect, validate, and verify one piece of "strong" identity evidence (*i.e.*, a driver's license, passport, or state identification card) and two pieces of "fair" identity evidence.

Approximately 85–90% of users who verify their identity with ID.me do so in minutes using the company's self-service pathway. To meet NIST requirements for identity evidence, ID.me's IAL2 pathway involves uploading an image of an identity document and a selfie, as well as additional checks in financial and telecommunications records to meet the NIST requirements for identity evidence. For remote proofing, NIST calls for either a physical or biometric comparison of the user to the strongest piece of identity evidence provided by that

---

[1] Consumer Financial Protection Bureau, *Who Are the Credit Invisibles? How to Help People With Limited Credit Histories* (2016), https://files.consumerfinance.gov/f/documents/201612_cfpb_credit_invisible_policy_report.pdf.

[2] Nat'l Inst. of Standards & Technology, *Digital Identity Guidelines: Authentication & Lifecycle Management*, NIST Special Pub. 800-63B (2017), https://pages.nist.gov/800-63-3/sp800-63b.html.

user. ID.me accomplishes this step by asking the user for a selfie and then comparing that selfie to the image on the government-issued identity document provided by the user, using one-to-one facial recognition technology. Where the images match, ID.me creates a verified digital credential that enables the user to seek services or benefits from ID.me's partner.

Supervised Remote: ID.me believes that the most equitable solution combines reliable algorithms with human-powered relief valves. The company's video chat pathway is exactly that: if the self-service flow is unable to confirm a user's identity, that user is given the opportunity to work with a human to complete the verification process. For the 10–15% of verifications that are not completed via the self-service pathway, ID.me automatically routes the user to complete an alternative verification pathway involving a video chat with one of the company's trained Trusted Referees.

NIST provides specific guidance on this pathway, which is called Supervised Remote identity proofing. In order to adhere to these guidelines, ID.me works with a user to upload either two "strong" or one "strong" and two "fair" pieces of identity evidence. The user must then demonstrate possession of that evidence in a video chat session. Examples of documents that can be provided by a user in a Supervised Remote pathway include driver's licenses, passports, veteran health ID cards, certificates of naturalization, and federally recognized tribal-issued photo IDs.

Some users are unable to provide sufficient evidence to meet NIST criteria via verification methods that rely on the user's presence in public records. These include international users (including members of the military stationed abroad and Americans living in U.S. territories or outside the United States), young adults, individuals without credit history, or individuals with recent name changes (*e.g.*, due to a recent marriage). As such, NIST enabled Supervised Remote as an option where the identity documents serve as standalone evidence to resolve, validate, and verify a user's identity, as long as that is done in the presence of a trained Trusted Referee. To provide additional flexibility, ID.me offers government agencies the option to enable users to choose to begin their identity-verification process in the company's Supervised Remote pathway and meet with a Trusted Referee in order to complete their verification.

To the company's knowledge, ID.me is the only Credential Service Provider that offers both Unsupervised Remote and Supervised Remote pathways to its government partners. The company's Supervised Remote pathway has been a key component in expanding access in its partnerships with government agencies. Originally launched by the U.S. Department of Veterans Affairs in 2019 to help veterans living overseas and veterans without credit records gain access to their benefits, ID.me's Supervised Remote pathway has now verified over 4.3 million users that likely would not have been able to access services using legacy verification methods.

Importantly, under ID.me's NIST-compliant identity-verification procedures, a user will not be denied a digital credential solely on the basis of a technological failure to match the image on a user's identification document with the selfie provided by that user. Rather, just as in an in-person setting, a user will be denied a credential only when a human agent—in this case, a

trained ID.me Trusted Referee—is unable to attest to the authenticity of the user's identification documents or collect enough verified evidence to meet NIST guidelines.

Under its agreements with its government partners, regardless of whether such denial is due to fraud prevention or a legitimate user who cannot meet the NIST requirements, ID.me does not receive compensation when a user is denied a requested credential. Instead, government partners pay ID.me only when a user successfully verifies their identity with ID.me or logs in with an existing or newly-issued credential. This compensation model ensures ID.me's incentives are aligned with producing successful results for the agency. This model is also consistent with ID.me's goal of simplifying the process of verifying and sharing identities online and is designed to support federal guidance encouraging steps to reduce the burden of identity verification on the public.[3]

Finally, it is important to recognize that ID.me has no role in determining a user's ultimate *eligibility* for services or benefits offered by ID.me's partners. NIST digital identity guidelines specifically prohibit identity proofing activities from determining "suitability or entitlement to gain access to services or benefits."[4] Rather, ID.me is responsible for verifying a user's identity and issuing a credential that promotes trust between an agency and a user: the agency will know with a high level of assurance that the individual claiming a set of personal identifying information is in fact that person. Each ID.me partner is then responsible for determining the user's eligibility for any such services and delivering those services to the user.

Expanding Access to Government Services During the COVID-19 Crisis

In the spring of 2020, Congress enacted sweeping legislation to provide much-needed support to Americans encountering financial hardship as a result of the ongoing COVID-19 crisis. State agencies looked for ways to accelerate benefits delivery at a time of urgent need. Many responded by relaxing or removing traditional eligibility requirements in unemployment assistance programs and relied on self-attestations of eligibility in the new pandemic unemployment assistance programs. In the months that followed, many state agencies struggled to efficiently distribute essential benefits to eligible claimants while detecting and thwarting potential fraud. In this unprecedented environment, numerous media reports highlighted difficulties state and local government agencies encountered in efficiently and reliably verifying the identities and eligibility of individuals seeking COVID-19-related benefits.

In particular, as has been widely reported, many government agencies struggled to rapidly scale-up the distribution of benefits without falling victim to malicious actors filing

---

[3] Office of Mgmt. & Budget, Memorandum for Heads of Executive Departments and Agencies: Enabling Mission Delivery through Improved Identity, Credential, and Access Management (2019), *available at* https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf.

[4] Nat'l Inst. of Standards & Technology, *Digital Identity Guidelines: Enrollment and Identity Proofing*, NIST Special Pub. 800-63A, 6 (2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf.

fraudulent claims.[5] With no other option to efficiently and reliably verify claimants' identities, states frequently resorted to a labor-intensive manual review process that often took weeks or months to complete.[6] This in turn led to significant backlogs of unprocessed claims, leaving many Americans unable to access the benefits to which they were entitled.

At a time when in-person services were still largely unavailable in most jurisdictions, state and local government partners came to ID.me for virtual pathways for Americans seeking critical government assistance. In many cases, ID.me's government partners tasked the company with verifying the identities of claimants presenting particular challenges, including those who had failed identity verification through legacy methods or were flagged as potentially fraudulent by government monitoring systems.

ID.me's earliest such partnership began in June 2020 when the Florida Department of Economic Opportunity sought the company's assistance in verifying the identities of claimants whose applications for benefits had been identified as potentially fraudulent by the agency's internal fraud tools. As was the case in many other states, agency staff were working to manually review and process each of these applications, significantly delaying the approval process and the provision of benefits to eligible claimants. In July 2020, the agency notified approximately 52,000 such claimants, who had been preliminarily identified as potentially fraudulent, that they would be able to verify their identities through ID.me's virtual pathways. Of those notified, only approximately 26% even attempted verification, with 86% of those users ultimately succeeding in verifying their identities. These users, who had been designated as potentially fraudulent by the agency, were verified and processed within 24 hours.

Following the success of the Florida pilot, the Georgia Department of Labor engaged ID.me to verify backlogged claims classified as "high-risk" by the agency. Beginning in mid-August 2020, the agency notified roughly 78,000 claimants whose applications were blocked due to internal fraud processes that they would be able to use ID.me to attempt to verify their identities. Only approximately 19,000 claimants who received this notification sought to verify their identities with ID.me, with more than 14,000 successful verifications. As was the case in Florida, these 14,000 claimants were able to successfully verify their identities and apply for benefits after being marked as potentially fraudulent by legacy verification processes.

Building on this proof of concept, ID.me entered into additional partnerships with government agencies across the country to provide secure authentication services in compliance with the NIST Digital Identity Guidelines. A list of ID.me's contracts with government partners, along with additional information regarding the company's services provided to its government

---

[5] Tim Henderson, *Fight Against Fraud Slows Payments to Unemployed*, Pew Trusts (Aug. 27, 2020), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/08/27/fight-against-fraud-slows-payments-to-unemployed.

[6] Phil Willon & Patrick McGreevy, *Newsom Vows Unemployment Claims Will Be Handled Faster*, Los Angeles Times (2020), https://enewspaper.latimes.com/infinity/article_share.aspx?guid=dfa86164-f3d2-4785-b134-458fe11a186e.

partners under these contracts, is included as Appendix A to this letter. Under these contracts, between March 1, 2020, and February 28, 2022, ID.me verified the identities of nearly 10 million users seeking unemployment benefits from state and local agencies.

Supporting Users Throughout the Identity-Verification Process

As ID.me's role in assisting government partners with the distribution of COVID-related benefits grew, the company continued to invest significantly to strengthen its capacity to support users seeking to verify their identities via the company's virtual pathways. In all events, ID.me's virtual pathways were designed to supplement existing verification channels offered by ID.me's state partners and were not intended to be the sole means of access for eligible beneficiaries. As noted above, however, these existing government channels—including traditional in-person verification—came under particular strain during the COVID-19 pandemic.

Among other investments, ID.me rapidly expanded the company's teams dedicated to supporting users who encountered difficulties in the identity-verification process. ID.me's Member Support teams are responsible for assisting all of the company's users, regardless of the particular credential they are seeking. Nonetheless, given the significant number of users seeking unemployment benefits during the pandemic, these teams regularly supported these users during this period. Additional information regarding ID.me's Member Support teams is included as Appendix B to this letter.

As a general matter, in working with government partners, ID.me aims to ensure that a significant proportion of an agency's users, ranging from 70–90% of users, are able to verify their identities and apply for benefits using ID.me's online pathways. In this way, ID.me can increase access to services via digital channels and reduce workload on government call centers and physical locations. However, ID.me also recognizes that some users encounter situations in which it is difficult to collect sufficient evidence online to adhere to NIST standards. With this in mind, ID.me has advocated for its government partners to provide alternative pathways to services, including in-person, mail, and call center options. Although these alternative pathways are generally provided by government partners, ID.me can also provide in-person identity-verification pathways where requested by its partners.

In particular, in connection with the provision of unemployment benefits, in November 2021, ID.me partnered with Sterling Identity, a leading provider of background screening and identity services, to create a solution for individuals to verify their identity in person at retail locations across the United States. This in-person verification network was designed explicitly to support increased access for individuals who do not own a phone, have limited or no reliable internet access, or who simply need help navigating digital interfaces. ID.me partners can now purchase the in-person identity-verification offering to help expand access to secure, easy-to-use identity verification. As with ID.me's virtual verification options, once a user verifies their identity in person, they can use their ID.me credentials to gain access to other services and benefits provided by ID.me's partners.

To date, the New Jersey Department of Labor and Workforce Development is the only ID.me government partner to take advantage of this in-person verification option. As requested

by the agency, to be eligible to verify in-person, users must be invited by the agency to schedule an appointment through ID.me at a Sterling Identity location convenient for them.[7] Between November 2021 and April 2022, users invited by the agency booked appointments at 26 locations in over 15 counties nationwide. A comprehensive list of the locations used to set up appointments is as follows:

- 228 East Route 59, Nanuet, NY, 10954 (Rockland County)
- 189 Berdan Ave, Wayne, NJ, 07470 (Passaic County)
- 13 Summit Square Center, Langhorne, PA, 19047 (Audubon County)
- 237 S Delsea Dr, Vineland, NJ, 08360 (Cumberland County)
- 4023 Kennett Pike, Wilmington, DE, 19870 (New Castle County)
- 136 Route 10, East Hanover, NJ, 07936 (Morris County)
- 1385 Hwy 35, Middletown, NJ, 07748 (Monmouth County)
- Lacey Mall 344 Rte 9 Ste 5, Lanoka Harbor, NJ, 08734 (Ocean County)
- 16 South Ave W, Cranford, NJ, 07016 (Union County)
- 295 Princeton Hightstown Rd, West Windsor, NJ, 08550 (Mercer County)
- 7151 Okelly Chapel Rd, Cary, NC, 27519 (Wake County)
- 7862 W Irlo Bronson Hwy, Kissimmee, FL, 34747 (Osceola County)
- 2474 Walnut Street Cary, NC, 27518 (Wake County)
- 1421 E Broad Street, Fuquay-Varina, NC, 27526 (Wake County)
- 4768 Broadway, New York, NY, 10034 (New York County)
- 1250 Bethlehem Pike, Hatfield, PA, 19440 (Montgomery County)
- 800 Denow Road, Pennington, NJ, 08534 (Mercer County)
- 157 Bridgeton Pike, Mullica Hill, NJ, 08062 (Gloucester County)
- 130 W Pleasant Ave, Maywood, NJ, 07607 (Bergen County)
- 3301 Rte 9 S, Rio Grande, NJ, 08242 (Cape May County)
- 10871 Bustleton Ave, Philadelphia, PA, 19116 (Philadelphia County)
- 209 W 29th St, New York, NY, 10001 (New York County)
- 7810 Gall Blvd, Zephyrhills, FL, 33541 (Pasco County)
- 105 E 34th St, New York, NY, 10016 (New York County)
- 1107 Mantua Pike, Mantua, NJ, 08051 (Gloucester County)
- 1134 S Black Horse Pike, Blackwood, NJ, 08012 (Camden County)
- 1229 Chestnut St, Philadelphia, PA, 19107 (Philadelphia County)

ID.me is committed to continuing to work with its government partners to provide alternative pathways to ensure that safe, secure, and effective identity verification is available to anyone who needs it. Combined with ID.me's self-service online and video chat processes, the availability of an in-person pathway has made ID.me the first secure and omni-channel identity-verification service in America.

[7] Sterling Identity maintains over 650 locations across the country, with the full list of locations available at https://sterlingidentity.com/locations/.

ID.me's Commitment to Equity, Privacy, and Security

ID.me is proud of its innovative identity-verification service that greatly expands Americans' access to digital channels by verifying their identities through one of the verification pathways described above. At the same time, ID.me is committed to implementing tools to prevent malicious actors from using stolen identities to commit fraud.

Among other systems, ID.me utilizes Duplicate Face Detection technology within its own system to prevent fraud. As the name suggests, this technology uses facial recognition to identify instances in which a selfie uploaded by a particular user appears to match a selfie previously uploaded by another ID.me user, which indicates that a single person may be attempting to verify different identities as their own. What distinguishes the company's use of this technology from other uses is that the company does not use external databases as part of this fraud control. Images are only compared against an internal database of photos previously uploaded to ID.me.

As the company has emphasized, Duplicate Face Detection technology is not used to verify the identity of ID.me's users.[8] Rather, as with users who are unable to verify their identities using ID.me's self-service process, the very small percentage of users whose photographs are identified by the company's Duplicate Face Detection technology for further review are offered alternative pathways to verify their identity, including through a video chat with a trained ID.me Trusted Referee. Users who do not pass through a facial recognition technology step in ID.me's process are only denied a credential when a trained ID.me Trusted Referee is unable to verify the authenticity of the user's identification documents.

Just as ID.me takes seriously its responsibility to prevent identity theft and fraud, the company is committed to safeguarding its users' personal information and empowering users to decide how that information is managed. Under the company's Privacy Policy, ID.me will not sell, rent, or trade personal information of users collected during the verification process. Instead, the company has committed to transferring a user's personal information only with their consent for use by third parties to verify a user's identity or group eligibility, and as required for the prevention of fraud.

Likewise, ID.me's approach to data retention aligns with the company's goal of providing individuals control over their personal information, while balancing compliance with external standards. As a general matter, as disclosed in the company's Privacy Policy, ID.me maintains evidence of an individual's verification—including any personal information, biometric information, or documentation—for audit and compliance purposes in accordance with NIST

[8] In contrast to the one-to-one system relied upon to compare two images uploaded by a user in the self-service identity-verification model described above, this technology compares images uploaded by a particular user to images uploaded by other ID.me users using a one-to-many system. As the company has elsewhere emphasized, in no instance does ID.me's facial recognition technology rely on external databases in order to verify the identities of its users or otherwise detect potential fraud within its systems.

standards and the company's external assessor's recommendations for up to three years after account closure. The company's fundamental goal in adopting this policy is to respect individuals' control over their data and privacy without creating a safe haven that criminals would exploit to cover their tracks by deleting evidence of their fraud.[9]

Further, as an element of its partnership with the agency, for users who are first verifying with ID.me to access information held by the Internal Revenue Service, ID.me automatically deletes any selfie and associated biometric information used as part of a successful verification within 24 hours. If a user does not complete the verification process after submitting a selfie and agreeing to the collection of biometric information, ID.me will delete their selfie and any biometric information after attempting to engage the user and encourage them to complete verification. If the user has not returned to complete the process within one week of the last engagement email sent to them, all data submitted by the user is deleted within the following 24 hours. All other ID.me users have the option to direct ID.me to delete their selfie and all associated biometric information at any time by visiting their ID.me MyAccount portal. Unless the company must retain such information to comply with the company's legal obligations or to help prevent fraud, ID.me complies with user deletion requests within seven days. Deletion of a user's selfie and biometric information does not impact the validity of the user's credential or verified status.

Estimates of Total Fraudulent Unemployment Claims

Throughout recent months, numerous government officials and private observers have highlighted the potentially unprecedented rate of improper payments for pandemic-related unemployment insurance ("UI") claims. Most notably, just last month, the Inspector General of the Department of Labor provided testimony to the U.S. Senate Committee on Homeland Security and Government Affairs indicating that the agency's own estimate of the improper payment rate for pandemic UI claims was 18.71%.[10] According to the Inspector General's testimony, at that rate, "at least $163 billion in pandemic UI benefits could have been paid improperly, with a significant portion attributable to fraud."

Moreover, this estimate was based on the regular UI program, which the agency concluded applied to only two of three key pandemic UI programs. Excluded from this estimate was data related to the Pandemic Unemployment Assistance program, for which the Inspector

---

[9] A copy of ID.me's Privacy Policy is available at https://www.id.me/privacy. Consistent with previous NIST guidelines, earlier versions of the policy provided that the company would retain biometric data provided by users for seven years. Other ID.me policies addressing biometric data retention are available at https://www.id.me/california, https://www.id.me/terms, and https://www.id.me/biometric.

[10] Pandemic Response and Accountability: Reducing Fraud and Expanding Access to COVID-19 Relief Through Effective Oversight: Hearing Before the Senate Comm. on Homeland Sec.& Gov't Affairs, 117th Cong. (2022) (Statement of Larry D. Turner), https://www.oig.dol.gov/public/testimony/20220317.pdf.

General noted the "risk of fraud and improper payments was even higher . . . because claimants could self-certify their eligibility" for benefits. As a result, the Inspector General testified that, based on his office's "audit and investigative work, the improper payment rate for pandemic-related UI payments is likely higher" than the 18.71% rate thus far reported by the agency.

This recent testimony is consistent with estimates from other government agencies and private experts. For example, according to the agency's most recent estimate, at least $20 billion in UI benefits paid out by the California Employment Development Department was fraudulent.[11] More troubling, an independent analyst working to assist states in helping to detect fake unemployment insurance claims has said that between 40% and 50% of the claims his group has analyzed "seem highly suspect."[12] Other analyses have likewise suggested that approximately 41% of pandemic-related UI claims went to people other than unemployed workers, which would equate to over $350 billion in fraudulent claims.[13]

As ID.me worked with its government partners to expand access to UI benefits across the country, the company saw firsthand that each fraudulent claim meant fewer dollars and longer waits for legitimate claimants. Failing to stop fraud also meant that legitimate claimants likely would be unable to file a claim because someone else had already filed a claim in their name. For these reasons, ID.me is committed to protecting the identities of its users while working closely with its government partners to prevent fraud. To that end, the company looks forward to continuing to work with Congress and other stakeholders to better understand the factors that contributed to the challenges described above while ensuring that all Americans have control over their online identities and the ability to safely and securely access the services they need.

* * *

Documents and information provided to the Committees may contain confidential business and financial information that ID.me considers proprietary and competitively sensitive. Disclosure of such information would harm ID.me and undermine the competitive marketplace. If the Committees should nonetheless consider the public release of such materials, we respectfully request that ID.me be given advance notice and an opportunity to

---

[11] Nick Cahill, *Fraudsters Scammed California Out of $20 Billion During Height of Pandemic*, Courthouse News Service (Oct. 25, 2021), https://www.courthousenews.com/fraudsters-scammed-california-out-of-20-billion-during-height-of-pandemic/.

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

[13] Rachel Greszler, *Excessive Pandemic Unemployment Benefits Are a Warning Against Unemployment Program Expansions*, Heritage Foundation (July 13, 2021), https://www.heritage.org/jobs-and-labor/report/excessive-pandemic-unemployment-benefits-are-warning-against-unemployment.

discuss the matter with you, so that we may explain ID.me's basis for objecting to public release of the materials.

Respectfully submitted,

Robert K. Kelner

cc: The Honorable James Comer, Ranking Member
Committee on Oversight and Reform

The Honorable Steve Scalise, Ranking Member
Select Subcommittee on the Coronavirus Crisis