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

June 17, 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 is a further response 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.

Today, we are producing documents numbered IDME-COR-SSCC-000001 to IDME-COR-SSCC-001720. Today's production includes documents identified as responsive to Requests 5, 6, and 8 included in your April 14 letter. In addition, this letter includes further information in response to those requests, as well as the company's response to supplemental requests from your staff related to Requests 3 and 4 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.

ID.me Policies and Efforts to Accommodate Requested Policy Modifications

In response to Request 3, in our initial response to your April 14, 2022 letter, ID.me provided hyperlinks to the current versions of the company's policies addressing the retention of biometric data collected through the company's identity-verification services. During a call on May 24, 2022, your staff requested any historical versions of these policies that would have applied to the company's collection and retention biometric data. In response to this supplemental request, the legacy versions that we have located of the ID.me policies previously provided in response to Request 3 are included as Appendix A to this letter.

As a further supplemental request, your staff requested information regarding instances in which ID.me has agreed to modify the company's standard data retention practices and/or its use of Duplicate Face Detection technology to detect and prevent potential fraud when providing services to government partners. In response to your staff's supplemental request, as of May 24, 2022, ID.me implemented the following modifications to its data retention practices and/or use of Duplicate Face Detection technology with respect to users seeking to verify their identities through the following government partners:

- <u>California Employment Development Department</u> – ID.me agreed to delete all selfies within 24 hours and all video recordings within 30 days. The company further agreed to suspend the use of Duplicate Face Detection, while also providing users the option to verify their identities through the company's Supervised Remote pathway. The "Direct to Trusted Referee" pathway creates a channel for a user to potentially complete the verification process without ID.me collecting or retaining any biometric data.

- <u>California Department of Public Health</u> – ID.me agreed to suspend the use of Duplicate Face Detection for users who verify their identities through the company's Supervised Remote pathway.

- <u>Department of Veterans Affairs</u> – ID.me agreed to delete all previously collected biometric data and to suspend the use of Duplicate Face Detection for users who verify their identities through the company's Supervised Remote pathway.

- <u>Federal Energy Regulatory Commission</u> – ID.me agreed to suspend the use of Duplicate Face Detection for users who verify their identities through the company's Supervised Remote pathway.

- <u>Internal Revenue Service</u> – ID.me agreed to delete all selfies within 24 hours and all video recordings within 30 days. The company further agreed to suspend the use of Duplicate Face Detection, while also providing users the option to verify their identities through the company's Supervised Remote pathway. The "Direct to Trusted Referee" pathway creates a channel for a user to potentially complete the verification process without ID.me collecting or retaining any biometric data.

- <u>Indiana Department of Workforce Development</u> – For users who have verified their identities, ID.me agreed to delete all selfies within 30 days.

- <u>Oregon Employment Department</u> – For users who have verified their identities, ID.me agreed to delete all selfies within 24 hours and all video recordings within 30 days. The company will provide the option for users to verify their identities through the company's Supervised Remote pathway. The "Direct to Trusted Referee" pathway creates a channel for a user to potentially complete the verification process without ID.me collecting or retaining any biometric data.

- <u>Pennsylvania Office of Unemployment Compensation</u> – For users who have verified their identities, ID.me agreed to delete all selfies and video recordings within 30 days.

- <u>United States Patent and Trademark Office</u> – For users who have verified their identities, ID.me agreed to delete all selfies within 24 hours. The company further agreed to suspend the use of Duplicate Face Detection, while also providing users the option to verify their identities through the company's Supervised Remote pathway. The "Direct to Trusted Referee" pathway creates a channel for a user to potentially complete the verification process without ID.me collecting or retaining any biometric data.

To date, the company has agreed to accommodate all such requests.

ID.me's Communications with the Internal Revenue Service

In response to Request 5, today's production includes communications between representatives of ID.me and the Internal Revenue Service ("IRS") regarding the company's use of Duplicate Face Detection technology as a fraud-prevention measure.

As explained in our prior correspondence, among other systems, ID.me utilizes Duplicate Face Detection technology within its own system to identify instances in which a selfie uploaded by a particular user appears to match a selfie uploaded by an already-verified ID.me user. In this way, ID.me uses Duplicate Face Detection to identify individuals who are attempting to claim multiple identities using images of the same face, which can be an indicator of fraud. Duplicate Face Detection identifies only a very small number of users (approximately 8 out of 10,000) for further review, all of whom are directed to a human reviewer for further analysis. If the reviewer determines that there is low likelihood of fraud, that user is offered an alternative pathway to verify their identity, including through video chat with a trained ID.me Trusted Referee.

Importantly, this fraud-detection measure is distinct from the use of facial recognition technology to compare two photos uploaded by a single user to verify the identity of that user, and Duplicate Face Detection technology is not used to verify the identities of ID.me users. Rather, the very small minority of users whose photographs are identified by the company's Duplicate Face Detection technology for further review are only denied a credential if a trained ID.me Trusted Referee is unable to verify the authenticity of the user's identification documents.

As reflected in the materials included in today's production, ID.me has clearly and consistently explained its use of Duplicate Face Detection as a fraud prevention measure to the company's partners at the IRS. Beginning in March 2021, shortly after the company operationalized the use of Duplicate Face Detection, ID.me provided agency representatives with detailed descriptions of the technology and its functionality, the date on which it was implemented, and information about its efficacy in detecting and preventing fraud. Throughout the spring of 2021, the company provided additional materials to the agency that clearly discussed the use of Duplicate Face Detection as a fraud-control measure. Later, when asked by agency representatives whether the company attempts to verify users' identities by reference to existing databases of images, the company correctly responded that it does not. By comparison, when the agency sought information regarding the company's Duplicate Face Detection technology in particular, ID.me representatives repeatedly confirmed that the company performs an internal review of user-uploaded selfies to detect circumstances in which a potential malicious actor may be attempting to fraudulently verify multiple identities in order to defraud the government.

During this period, ID.me was continuing to work closely with its state government partners to combat widespread fraud in connection with the provision of pandemic-related unemployment insurance. Mindful that malicious actors would attempt to use information regarding the company's fraud-prevention measures to circumvent those measures, ID.me's public-facing statements regarding its technology have generally been tailored to focus on the identity-verification process itself. These statements have thus offered less detail regarding the use of Duplicate Face Detection technology as a separate, internal fraud-prevention measure. In some instances, because the agency was aware of ID.me's use of Duplicate Face Detection technology, IRS officials sought clarification regarding the company's emphasis on its exclusive use of one-to-one technology to verify users' identities in its public-facing communications. In response, ID.me repeatedly confirmed to the agency that it does not use Duplicate Face Detection technology to verify a user's identity and instead uses the technology only to detect and prevent fraud.

ID.me's Use of Commercially Available Facial Recognition Technology

ID.me uses commercially available facial recognition models for both the company's one-to-one identity verification process (*i.e.*, the comparison of a selfie provided by a particular user to the photo included the identity document provided by that user) and the separate Duplicate Face Detection technology fraud-detection measure (*i.e.*, the comparison of a selfie provided by a particular user to other selfies previously uploaded by ID.me users). As previously explained, the company does not use external databases as part of the Duplicate Face Detection process, and images provided by ID.me users are compared only against an internal database of photos previously uploaded to ID.me. In response to a supplemental request from your staff, a flow chart describing ID.me's identity-verification process is included as Appendix B to this letter.

For one-to-one identity verification, ID.me currently relies on facial recognition technology supplied by Paravision. As described in the National Institute of Standards and Technology's October 2021 Facial Recognition Vendor Test, the Paravision technology is among the most accurate technologies currently available in the United States.[1] Previously, the company relied on Rekognition software provided by Amazon Web Services for both one-to-one identity verification and Duplicate Face Detection. Though the company continues to rely on

[1] *See, e.g.*, "Paravision Raises the Bar in Latest NIST FRVT 1:1 Report," Paravision (Feb. 2022), https://www.paravision.ai/news/paravision-face-recognition-raises-the-bar-latest-nist-frvt-11/; National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 7: Identification for Paperless Travel and Immigration* (Oct. 28, 2021), https://pages.nist.gov/frvt/reports/travel/frvt_travel_report.pdf; "Paravision Delivers #1 U.S. Performance in New NIST Report on Face Recognition and Paperless Travel," Paravision (July 2021), https://www.paravision.ai/news/nist-frvt-paperless-travel-july-2021/.

Rekognition for its Duplicate Face Detection, the company is exploring employing Paravision for this application, in addition to the one-to-one identity verification application.

These AI-based facial recognition models are essentially "off the shelf," in that ID.me itself has not built or trained the models. Although the company can provide feedback on the models' performance to the respective providers, ID.me does not have access to any databases used to train the facial recognition models or general data about the models' error rates.

Nonetheless, throughout the last year, ID.me has conducted two analyses of the performance of its Unsupervised Remote identity-verification pathway to attempt to identify any relationship between instances in which users have been unable to verify their identities and those users' skin tones. Today's production includes copies of reports summarizing the findings and methodology of these analyses. As these reports indicate, neither analysis identified statistically significant evidence of a relationship between a user's failure to verify their identity through the Unsupervised Remote pathway and that user's skin tone.

ID.me's Investor-Facing Communications Regarding Fraud Prevention

Also included in today's production are presentations to the CyberSecurity and Risk Committee of the ID.me Board of Directors between January 2020 and February 2022. This Committee includes members of ID.me's Board of Directors, which includes representatives of a number of the company's largest outside investors. These presentations discuss ID.me's fraud prevention efforts, including internal staffing updates, partnerships on fraud prevention workflows, and the use of technological tools to reduce fraud.

Notably, the work of ID.me's fraud prevention team discussed in these presentations is not limited to identifying efforts by malicious actors to fraudulently obtain access to benefits and services provided by ID.me's public and private partners. Rather, the fraud-prevention efforts described in these materials also refer to the company's efforts to identify and prevent the misuse of confidential information provided by users to ID.me. To our knowledge, ID.me generally does not provide other materials to the company's investors that specifically discuss the company's fraud-detection capabilities, including the use of Duplicate Face Detection technology.

Estimated Pandemic-Related Unemployment Fraud

Finally, on our May 24 call, your staff requested additional information regarding ID.me's public statements addressing the potential total value of COVID-era unemployment insurance ("UI") claims that may have been fraudulent. As indicated in our April 28, 2022 letter, ID.me's understanding of the extent of improper payments for pandemic-related UI claims draws on a number of sources, including public statements by state and federal officials responsible for administering and overseeing UI programs, estimates put forward by third-party analysts assisting state governments in detecting potential fraud, and the company's own observations of the incidence of potential fraud through its efforts to provide identity-verification services to state government partners.

In particular, numerous state government agencies responsible for administering UI programs have released preliminary estimates of the value of improper payments processed through their programs in connection with COVID-era UI claims.[2] These preliminary estimates, as well as the broader estimates described in our April 28 letter, are consistent with ID.me's own observations regarding the significant decline in new or renewed UI claims upon the introduction of identity-verification methods meeting current National Institute of Standards and Technology standards in states across the country. Though it is of course impossible to estimate the total amount of improper payments with perfect precision, ID.me's public statements reflect the company's best understanding of the incidence of potential fraud in connection with pandemic-related UI programs nationwide. The company looks forward to continuing to work with its government partners and other stakeholders to combat fraud while expanding access to vital government services.

* * *

Documents and information provided today 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 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

[2] *See, e.g.*, Jaclyn Diaz, *Michigan paid up to $8.5 billion in fraudulent jobless claims during the pandemic*, Nat'l Pub. Radio (Dec. 30, 2021); Adam Beam, *California's unemployment fraud reaches at least $20 billion*, L.A. Times (Oct. 25, 2021), https://www.latimes.com/california/story/2021-10-25/californias-unemployment-fraud-20-billion; Bob Christie, *Scammers got nearly 30% of Arizona virus unemployment pay*, Associated Press (Sept. 30, 2021), https://apnews.com/article/coronavirus-pandemic-business-health-arizona-1f9f1361199f19f7cdc4279a546a37b1.