Montana Economic Affairs Interim Committee

Statement for the Record- 2/9/2022

(Pete Eskew, ID.me General Manager, Public Sector)

Introduction

Chairman Bogner, Vice Chair Harvey, Members of the Committee, thank you for this opportunity to participate in an important discussion on key privacy and security policy matters facing Montana and the nation. We sincerely appreciate your time and consideration of these important issues and look forward to working with you to protect your constituents from identity theft while enabling access to government programs.

ID.me is deeply committed to access, equity, security, and privacy. Since 2013, we have worked directly with the National Institute of Standards and Technology (NIST) to advance a consumer-centric model of identity verification where individuals – not data brokers or credit bureaus – get to decide how their data is shared.

All uses of facial recognition are internal to ID.me and do not involve government agencies, law enforcement, or public photos. Our use of the technology is far different from Clearview AI, a facial recognition tool designed to allow law enforcement to take a photo and to find the true identity of that person. We don't do that. Our goal is to put you in control of your own data. And to prevent people who are not you from taking control of your data. That is it.

We have been praised for innovating to increase access and equity over the years. First, at the Department of Veterans Affairs, where we created a new and alternative pathway that allowed people who live overseas, the unbanked, and homeless populations to prove their identity online for the first time ever. Today, we support the State of Montana, 10 federal agencies, 29 additional state governments, and 38 healthcare organizations.

In Montana, ID.me partnered with the Montana Department of Labor and Industry (DLI) beginning in November of 2020 to assist with identity verification for unemployment insurance (UI). To date, ID.me has verified 39,077 claimants on behalf of Montana DLI. Of those claimants, 31,440 (80.5%) verified via ID.me's unsupervised verification flow. 7,637 (19.5%) of those claimants verified via ID.me's supervised Trusted Referee, or video chat, verification flow.

A. Fraud Exploded During the Pandemic

Twenty-seven states turned to ID.me to enable access to benefits and to defeat organized crime during the pandemic. I'd like to share how our access and security features proved critical to ensuring aid flowed to our most vulnerable communities while preventing identity theft. The Federal Trade Commission (FTC) reported that identity theft tied to government benefits increased by 2,920 percent year over year. Crime rings breached Vertafore and Automatic Funds Transfer, the contractors for the nation's largest DMVs. T-Mobile was breached repeatedly during the pandemic. Criminals not only had hordes of stolen personal data – but proof that they were you.

B. Access Is Critical

When we started supporting state workforce agencies in the summer of 2020, many, like the California Employment Development Department (EDD) had completely shut down due to fraud. Repeatedly, ID.me enabled these agencies to re-open and to get critical aid flowing again.

Immediately after deploying in California and Arizona, we were hit with – and defeated – multiple cyberattacks from Nigeria, Russia, and China. This opening salvo proved the first round of a fight we have led to protect America from our adversaries. It continues today at this very moment. Fraud prevention and access are inextricably linked.

We have verified more than nine million people for unemployment benefits with more than 1.5 million people verifying through our video chat verification pathway. ID.me is the only certified Credential Service Provider in the United States with a Supervised Remote (video chat) offering. We developed this capability to ensure all eligible users can verify their identity online.

While ID.me's Unsupervised Remote workflow has industry-leading pass rates between 80 - 87%, depending on the particular application, we noticed that records-based validation requirements effectively precluded individuals without credit history from proving their identity online. In practice, this meant that minority communities and women, who are more likely to have their names recorded inaccurately in records due to increased propensity for name change, suffered lower access rates. We found that state of affairs to be deeply unjust, so we resolved to fix it.

We listen to our partners each and every day so that we can learn about their issues and work together to resolve them. For example, in March of 2021, Montana DLI and ID.me began working together to add Federally Recognized Tribal IDs to ID.me's list of acceptable primary identity verification documents. ID.me's product team updated the verification process, and by April of 2021, Federally Recognized Tribal IDs could be accepted as a primary document for identity verification in accordance with the NIST 800-63-3 publication. Montana DLI was instrumental in drawing attention to this necessary product update and ensuring that the Native American population had equitable and secure access to state unemployment benefits.

C. Security - ID.me follows and is audited against federal standards

ID.me follows the federal government's security and privacy standards set by NIST, the Office of Management and Budget (OMB), and the General Services Administration. We adhere to:

- NIST 800-63 Federal Digital Identity Guidelines
- OMB Memorandum M-19-17, which calls for "federally provided or commercially provided shared services" to "deliver identity assurance and authentication services to the public."
- NIST 800-53 – with a FedRAMP certification, which shows our platform is secure.

During the pandemic, we found the selfie step to be a critical control to prevent identity theft. When we activated the selfie, estimated fraud rates dropped by 10 - 29% as a percentage of overall claims applications. Four states have credited us with preventing $210 billion in fraud.

D. ID.me is Central to Access and Security While Combating Fraud

There are two things you need to know about ID.me and they are both true at the same time:

1. We are more equitable and secure than any other digital solution in America.
2. We are not the right solution for everyone – we operate within the boundaries of societal constraints.

Most federal and state agencies offer alternative pathways and in-person services for access to benefits. To use a metaphor, we are a digital fast lane option to expedite transactions but people can use other access routes. However, state workforce agencies were so overwhelmed during the pandemic that many turned completely to ID.me to verify everyone.

We would never advocate for a digital only approach. Our goal in the states was to take 90% of individuals out of the manual flow. There are structural inequities like digital skills, phone ownership, photo identification, and internet access that form constraints within which we operate. It will take a whole of society effort to bridge the gap to these communities.

To ensure that we provide equitable verification options for all U.S. citizens, ID.me launched an in-person verification solution this past summer. We believe that everyone should have the opportunity to securely verify their identity and then take their verification to any other agency that they desire. Later this month, Montana DLI and ID.me are launching a pilot program for in-person verification at the Billings Job Services Workforce Center. This in-person verification option will allow claimants to make an appointment at the Billings Job Services Workforce Center and verify their identity in-person. If successful, Montana DLI may expand the in-person verification solution to additional Job Services Workforce Centers in Montana.

E. The Opportunity and Challenge We All Have Before Us

Our country is at a major inflection point; the question is how to bring about an advancement that people may not feel ready for and one that asks hard questions, but one that also meets an urgent need and delivers for Americans. How can we balance the trade-offs between new ways of verifying – taking a selfie – versus allowing domestic and foreign criminal organizations that have innovated themselves to abuse hundreds and thousands of Americans' identities for their own gain. And that ultimately is a policy question.

<u>Committee Questions</u>

1. **ID.me's biometric privacy policy states that you will share or disclose user's biometric information to "comply with legal obligations or applicable, to respond to legal process (such as a subpoena, warrant or civil discovery request), to cooperate with law**

enforcement agencies concerning conduct or activity that we reasonably and in good faith believes may violate federal, state, or local law." Does ID.me [id.me] always require a criminal subpoena or warrant prior to sharing/disclosing user's biometric info in cooperation with a criminal search by law enforcement? If not, are there any legal standards (probable cause, reasonable suspicion etc.) which ID.me [id.me] always requires before sharing/disclosing info in cooperation with a criminal search by law enforcement?

ID.me Response:

ID.me requires a valid subpoena, warrant or similar court order to share information with law enforcement. ID.me will share information with state agencies regarding identity theft and fraud. State agencies may involve law enforcement at their discretion.

2. **How many criminal searches by federal and state law enforcement has ID.me [id.me] cooperated with by sharing or disclosing user's biometric info?**

ID.me Response:

To date, ID.me has received 35 subpoenas and three warrants.

3. **Can ID.me [id.me] provide the committee a list of all law enforcement search requests made and all the requests ID.me [id.me] has cooperated with by sharing user's biometric info?**

ID.me Response:

Law enforcement search requests, including subpoenas and warrants, are typically issued pursuant to an active investigation into a crime. As such, the governmental issuing body requests that the existence of the subpoena or warrant not be disclosed, and in some cases they forbid such disclosure as such disclosure could interfere with the enforcement of criminal laws and risk exposing personal identifiable information of individuals who are ultimately not charged with a crime.

4. **Does ID.me [id.me] maintain documentation of data-share agreements, Memorandums of Understanding etc. to share/disclose user's biometric info (including photos) with any state or federal law enforcement agencies or databases? If yes, please disclose these documents to the committee for inspection. If no, does ID.me [id.me] always cooperate with criminal searches by law enforcement on a case-by-case basis or are there any standing arrangements to facilitate searches?**

ID.me Response:

No. ID.me will only share data with law enforcement agencies with a valid subpoena, warrant or other applicable court order, or as part of an investigation into an identity theft or fraud case only at the specific agency where the ID.me account was involved.

When ID.me is served with documentation relating to a criminal search, the ID.me legal team reviews the subpoena, warrant or similar court order to determine what information ID.me is legally required to provide. The ID.me legal team reviews all documents produced by the company in response to legally compelled document production requests prior to the release of such documents to ensure that the response submitted is not overbroad and only contains sensitive or confidential information specifically requested.

ID.me does not contribute data in bulk to any state or federal law enforcement databases. And, just to reiterate, ID.me does not sell data.

5. **Why does ID.me [id.me] store user's biometric information for up to seven and a half years after users close their account? Do the same privacy protections apply to stored data?**

ID.me Response:

The subject contract with Montana was performed in accordance with NIST Special Publication 800-63-2, Electronic Authentication Guideline, which required a retention period of seven years and six months.

Users may request the deletion of their personal information used in connection with a verification, and such requests will be completed upon the expiration of the retention schedule. Leading privacy legislation, such as the California Consumer Privacy Act, also makes exceptions to deletion requests when the risk of identity theft and fraud is high. Laws written to protect consumer privacy should not be abused by identity thieves to hide their tracks, and leading privacy frameworks account for this scenario.

ID.me's privacy policy ensures the user is in control of their data (https://www.id.me/privacy). The company also provides a Privacy Bill of Rights (https://insights.id.me/privacy-bill-of-rights/).

6. **We recently noted the federal government's intention that citizens use facial recognition through ID.me [id.me] to pay their taxes online. Please provide details on how this massive amount of facial recognition data will be stored and how ID.me [id.me] intends to share this data.**

ID.me Response:

ID.me currently collects biometric data as part of our NIST Identity Assurance Level 2 verifications for both our state and federal partners - including the IRS - using facial recognition technology. NIST 800-63A calls for "physical or biometric comparison of the photograph on the strongest piece of evidence to the applicant."

ID.me is certified against NIST 800-53 with a FedRAMP Authority to Operate from the General Services Administration. This certification speaks to the rigorous technical and policy controls ID.me adheres to in order to ensure data security.

Data is encrypted and stored by ID.me in a way that cannot be accessed by any other entity besides ID.me. No third party organizations, including government agencies, have access to ID.me's database. The information provided by ID.me users for the purposes of verifying their identity with government agencies is securely retained by ID.me. Biometric data is not shared with government agencies as part of the verification process.

Further, ID.me does not share biometric data with any government agency, absent the receipt of a subpoena, warrant, or similar court order or as part of an investigation into an identity theft or fraud case only at the specific agency where the ID.me account was involved.

7. Do you share Montanans data with advertisers?

ID.me Response:

ID.me does not share data with advertisers absent consent, through an opt-in process, from the individual to whom such data pertains. ID.me never sells data to advertisers. ID.me provides individuals with complete control over their own information. For example, if a veteran wishes to prove he served in the military to get a free ticket to Busch Gardens, then we enable that veteran to prove military service without over disclosing sensitive information such as social security numbers that are on the Form DD 214.

It is each individual's right to control their own information and to share it as they see fit. In the same way that Visa doesn't sell your money, ID.me doesn't sell your data. We help people prove their identity attributes rapidly when they want to.

8. Please provide ID.me's privacy policy that is currently in use for Montanans data.

ID.me Response:

https://www.id.me/privacy