ID.me

Building the Identity Layer of the Internet
Blake Hall—CEO and Founder

Social Security Advisory Board
March 26, 2021
Agenda

ID.me Overview
Expanding Access
Fighting Fraud
Feedback & Discussion
Executive Summary

The Identity Layer for the Internet:

**Digital** applications are proliferating, but identity and login verification are still point solutions.

**Friction** tied to point login and verification workflows places an enormous tax on commerce.

**Identity** as a platform streamlines every workflow in society the same way Visa solved payments making this safe & simple for individuals.
State of the ID.me Identity Network

- **39M+** Members  
- **75K** Daily Sign-ups  
- **7** Transactions/User  
- **405** Organizations

- **Leading The Way**
- First identity network in America to make digital credentials portable across government, healthcare, and commerce.
- Deeply entrenched within 405 organizations as a critical tool users leverage to login or verify
- Treated by customers as a valuable channel to increase service delivery
- Contracts with 22 states using ID.me for PUA unemployment verification. ID.me has blocked 1.2M fraudulent claims through 1/31, sparing taxpayers a loss of over $24 billion.
CERTIFIED
Certified NIST 80063-3
IAL2/AAL2 Credential
Service Provider (CSP) with
Unsupervised & Supervised
Remote proofing

SECURE
Leverages remote
verification of IDs, MNO
data, fraud algorithms,
& FIPS 140-2 level
encryption

PORTABLE
Delivers Identity-as-a-
Service through
federated identity
protocols: SAML 2.0,
OAuth 2.0, OIDC
An Identity Network Built for Consumers
Digital Identity is Broken

Portable logins aren’t trusted and trusted logins aren’t portable

Login with Facebook

ID.me fills the Trusted & Portable Role

Login with Google

Login with Amazon

AT&T, Citibank, Wells Fargo

Credential Identity & Authentication
At the same time, identity underpins literally every transaction in society.
ID.me provides online NIST 800-63-3 IAL2 and AAL2 options for all users -- even for those users who don’t have a presence in records.

### MOST COMMON

**ONLINE, SELF-SERVE**

### RELIEF VALVE

**VIRTUAL IN-PERSON PROOFING VIA VIDEO CONFERENCE CHAT WITH AN ID.ME TRAINED CALL CENTER AGENT**

### OPPORTUNISTIC

**IN-PERSON PROOFING WITH TRUSTED REFEREE**

**If user hits a roadblock verifying their identity online.**

**Trained agent proofs user to NIST IAL2 via video chat**

**User goes to a Trusted Referee location and proofs in-person**
ID.me provides an orchestration platform for validation, verification, and authentication that partners can configure according to risk.

<table>
<thead>
<tr>
<th>Verification</th>
<th>Validation</th>
<th>Multi-Factor Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government ID (Strong)</td>
<td>Credit Bureaus</td>
<td>Enhanced SMS</td>
</tr>
<tr>
<td>Subscription</td>
<td>Mobile Network</td>
<td>Native App Push</td>
</tr>
<tr>
<td>Phone/Telecoms (Strong)</td>
<td>Operators/Telecoms</td>
<td>Native App TOTP</td>
</tr>
<tr>
<td>Facial Liveness (Strong)</td>
<td>DMVs</td>
<td>FIDO U2F Tokens</td>
</tr>
<tr>
<td>Video Proofing (Strong)</td>
<td>State Licensing Data</td>
<td>Fraud/Device Intelligence Feeds</td>
</tr>
<tr>
<td>Knowledge Based Verification (Fair)</td>
<td>Many Additional Registration Authorities</td>
<td></td>
</tr>
</tbody>
</table>
Organizations select from a menu of turnkey policies to map the appropriate level of legal ID proofing based on risk and requirements.

KBA Replacement: Document Verification OR Telecom Verification

Fortified Identity: Document Verification AND Telecom Verification OR Face Liveness

NIST 800-63-3 IAL2: Document Verification AND Telecom Verification AND Selfie with Matching
Identifying Special Populations and Roles

ID.me is uniquely architected to validate if a given person is also:

- a member of the military/veteran
- a student
- a teacher
- a first responder
- low-income
- a healthcare provider
- an employee
**ID.me provides configurable authentication policies based on risk and attributes**

<table>
<thead>
<tr>
<th>Strong Validation, but Weak Verification</th>
<th>Strong Validation &amp; Strong Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Group Verification</td>
<td>6. NIST 800-63-3 IAL2/AAL2</td>
</tr>
<tr>
<td>2. SCRA Monitoring</td>
<td>7. EPCS Identity Proofing</td>
</tr>
<tr>
<td>3. Document Verification</td>
<td></td>
</tr>
<tr>
<td>4. KBA Replacement</td>
<td></td>
</tr>
<tr>
<td>5. Fortified Identity</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Clients</strong></th>
<th><strong>Clients</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail, Automotive, Subscription Services</td>
<td>Federal, State, Local Government, Healthcare</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td>Verify group affiliation to provide exclusive access to benefits</td>
<td>NIST 800-63-3 identity proofing and authentication, combined with medical provider verification</td>
</tr>
</tbody>
</table>

**Product Variations**
- a. Military
- b. Student
- c. Teacher
- d. First Responder
- e. Government Employee
- f. Company Employee
- g. Nurses
- h. Doctors
- i. Income

**Solution**
- Automated identity verification flow where user can verify identity using Mobile Identity Verification OR Document Verification

<table>
<thead>
<tr>
<th><strong>Product Variations</strong></th>
<th><strong>Product Variations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Military</td>
<td>a. ID.me CSP</td>
</tr>
<tr>
<td>b. Student</td>
<td>b. White-Label CSP</td>
</tr>
<tr>
<td>c. Teacher</td>
<td></td>
</tr>
<tr>
<td>d. First Responder</td>
<td></td>
</tr>
<tr>
<td>e. Government Employee</td>
<td></td>
</tr>
<tr>
<td>f. Company Employee</td>
<td></td>
</tr>
<tr>
<td>g. Nurses</td>
<td></td>
</tr>
<tr>
<td>h. Doctors</td>
<td></td>
</tr>
<tr>
<td>i. Income</td>
<td></td>
</tr>
</tbody>
</table>

**Solution**
- NIST 800-63-2 LOA3 or NIST 800-63-3 IAL2/AAL2 credentialing flow. Combines attribute validation, device verification, document verification, with biometric matching, or Virtual In-Person or In-Person proofing

<table>
<thead>
<tr>
<th><strong>Product Variations</strong></th>
<th><strong>Product Variations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. ID.me CSP</td>
<td>a. ID.me CSP</td>
</tr>
<tr>
<td>b. White-Label CSP</td>
<td>b. White-Label CSP</td>
</tr>
</tbody>
</table>

**Solution**
- NIST 800-63-3 identity proofing and authentication, combined with medical provider verification

**Product Variations**
- a. ID.me CSP
ID.me Offers Complete MFA Capabilities

**Enhanced SMS**: ID.me offers fortified SMS by verifying the enrolled device during proofing and checking the device during subsequent logins.

**Phone call**: 20% of adults over the age of 65 do not own a cell phone. Users can verify using a 6-digit security code sent by voice to landline.

**Code generator**: Users can use a code generator app on iOS or Android. Code generator apps work even when there is no cell signal.

**ID.me native app**: With the ID.me Wallet app, users will receive a push notification which prompts the user to authenticate via touch ID or PIN code.

**Security key**: Users can use FIDO U2F security keys as a second factor. The physical token is bound to the user’s identity.
Users who go through ID.me’s Unsupervised Remote flows must have a phone with tenure, a valid government ID with photo, and pass a selfie match step.

Market for identity verification is moving from knowledge-based methods to possession and biometric based methods.

Knowledge-Based Verification (KBV)
- Inherently weak.
- Answers available on dark web.

Driver’s License or Passport

Selfie with Liveness

Device & Telecom Verification

To prove with confidence that the user is who they claim to be, the user should prove that they physically possess something that reflects their identity – something with a reputation built over time or is hard to forge.
Face Match (1:1) enhances privacy and prevents identity theft while Face Surveillance (1:Many) is much more problematic
ID.me provides a federally certified video chat solution so all users can verify

ID.me’s Virtual InPerson Proofing ensures all users can prove their identity online in minutes at different assurance levels:

- Users who present a high-risk so a recorded video session would provide a strong deterrent to fraud
- Users who are recent immigrants
- Users whose information is entered into financial and/or utility records inaccurately
- Users with a limited credit history with credit bureaus
- Users with a limited history in utility records
- Users who are uncomfortable with technology and require additional assistance
No Identity Left Behind

Users who don’t have credit history or who need help can use their government ID and video chat to verify their identity in minutes.

- NIST 800-63-3 Supervised Remote certified
- Individuals can use two Primary IDs OR one Primary ID and two Secondary documents
- Sessions are recorded for audit purposes
- Agents are all US-based
ID.me provides trust and access to the digital and physical application layers without tracking consumer behavior and data within those apps.

Surveillance State

Voyeur State

Trust Layer
Fighting Fraud
ID.me - Fighting Fraud

Primary Fraud Vectors

Social Engineering: legitimate owner of identity (victim) unwittingly helps the attacker perpetrate fraud

Secondary Phone: criminal uses breached PII to register a phone in the victim’s name with the telecom to defeat carrier verification

Fraudulent Documents: suspicious documents uploaded appear to be clearly fabricated, edited, or altered

Mitigating Controls

Bolster Messaging: ID.me notifies individuals at their phone number of record that their identity was used at an agency—similar to banks and credit cards

Device Verification: ID.me monitors for a single device and/or IP tied to multiple verified accounts, different phone numbers and/or SIMs

Machine Learning Algorithms: ID.me monitors for duplicate document images and numbers, and leverages ML/AI to detect fabricated elements

19 states are currently using ID.me for PUA unemployment verification

Blocked an estimated 895,974k fraudulent claims through 1/31

Prevented over $17 billion in taxpayer loss to fraudulent payments

900% Increase in dark web traffic related to ID.me since Oct-2020

21

900% Increase in dark web traffic related to ID.me since Oct-2020

Prevented over $17 billion in taxpayer loss to fraudulent payments

900% Increase in dark web traffic related to ID.me since Oct-2020

21

900% Increase in dark web traffic related to ID.me since Oct-2020

Prevented over $17 billion in taxpayer loss to fraudulent payments

900% Increase in dark web traffic related to ID.me since Oct-2020

21

900% Increase in dark web traffic related to ID.me since Oct-2020

Prevented over $17 billion in taxpayer loss to fraudulent payments

900% Increase in dark web traffic related to ID.me since Oct-2020

21

900% Increase in dark web traffic related to ID.me since Oct-2020

Prevented over $17 billion in taxpayer loss to fraudulent payments

900% Increase in dark web traffic related to ID.me since Oct-2020

21

900% Increase in dark web traffic related to ID.me since Oct-2020

Prevented over $17 billion in taxpayer loss to fraudulent payments

900% Increase in dark web traffic related to ID.me since Oct-2020

21

900% Increase in dark web traffic related to ID.me since Oct-2020

Prevented over $17 billion in taxpayer loss to fraudulent payments

900% Increase in dark web traffic related to ID.me since Oct-2020

21
Types of Fraud we're seeing across our network

- **Basic Identity Theft (18 - 20% of Claims):** an attacker leverages stolen personal data to file a claim in the victim’s name.

- **Social Engineering (7.5 - 10% of Claims):** an attacker convinces a victim they are verifying their identity for a job or to get prize money.

- **Face Matching (2 - 2.5% of Claims):** an attacker holds up a picture, video, and, increasingly a computer generated 3-D printed mask of the victim’s face.

- **Prisoner Fraud (Unknown % of Claims):** incarcerated individuals who are ineligible to file claims do so anyway.

- **First-Party Fraud (Unknown % of Claims):** an attacker convinces a mule -- an individual who knowingly aids the attacker -- to let the attacker file a claim in the mule’s identity in exchange for a cut of the claims payment. The mule then contacts law enforcement and pretends to be a victim of identity theft.

- **Synthetic Identity Theft (Unknown % Claims):** an attacker creates a fictional identity in credit records and uses the fake or synthetic identity to file a claim for an identity that does not exist.
Social engineering attacks **7.5 – 10%** of gross claims volume across our state partners.

- Industrial scale telemarketing style operation with specific scams targeted at specific demographics (e.g. prize money scams to the elderly, business scams to middle-aged business owners, and job scams targeted against young people).

- **50%+** of total out of state applicants are fraud via this attack vector.

- Organized crime is succeeding in manipulating victims about **20%** of the time.
Fraudsters are even wearing masks to evade us
Criminals are increasingly using computer generated 3-D masks to attempt to commit identity theft but they have not been successful
Dark web chatter validates the effectiveness of our controls
Meanwhile, SBA is getting hammered with fraud tied to PPP
We are defending American agencies against nation-state attacks
Thank You!

Blake Hall  
Founder & CEO  
O: 703-639-0052  
blake@ID.me  
Twitter: @blake_hall

About ID.me

ID.me is the next-generation digital identity platform that enables trusted and convenient interactions between individuals and organizations. ID.me provides seamless online identity verification for government, financial services, and healthcare to facilitate access to high value services online and keep them safe from fraud. The platform brings together best-in-class identity and fraud vendors into a comprehensive, easy-to-deploy solution for partners. For more information, visit www.ID.me.