Secretaries’ Innovation Group
Agenda

Origination of Pandemic Fraud

Solution - NIST 800-63-3

Recommendations
**Urgent Political Action in 2020 Created Opportunity for Identity Fraud**

**MAR 27, 2020**  
CARES Act Enacted to Provide Pandemic Relief  
Total spent on PPP - $800B  
Total spent on EIDL - $400B  
Total spent on UI - $900B  
Total spent: $5T

**JUN 29, 2020**  
Florida

**SEP 3, 2020**  
Arizona

**MAR 26, 2021**  
New Jersey

**AUG 11, 2021**  
DOL Provides $140M to the States to implement NIST-compliant identity proofing, specifically IAL2/AAL2

**JAN 1, 2022**  
EIDL closed down

**MAY 31, 2021**  
PPP Closed down

**DEC 27, 2021**  
Pandemic Response Accountability Committee: To combat these sophisticated identity fraud schemes, the federal government must stand up robust systems to minimize identity fraud in its programs.

**MAR 26, 2021**  
ID.me’s NIST Compliant ID verification Adoption - Publicly credited with preventing over $238B in improper payments in 5 states (Now supporting 27 state workforce agencies)

**DEFENSIVE MEASURES**

**MAR 27, 2020 - JUN 29, 2020**  
Invitation for Fraud  
EIDL, PPP, and PUA Initially Relied on Self-Certification

**AUG 13, 2020**  
Georgia

**OCT 1, 2020**  
California

**JUN 13, 2022**

**Confidential & Proprietary Information of ID.me**
The response to the pandemic created the perfect storm

- Fast paced policy action
- Monetary Rewards
- Outdated technology in underinvested agencies

FTC reports 2,920% increase in ID theft in 2020
Trillions of dollars available for claimants
Systems unprepared

ID theft has soared
Victims in multiple categories
Criminals use the dark web to actively sell info & discuss verification methods thwarting their efforts

Arkansas do idme???
May 07, 2021 12:01:38

At all bru…they don’t use Idme…eat up brother
May 07, 2021 12:04:06

No IDme for Arkansas
May 07, 2021 13:22:26

Who can unlock, locked FL UI? It requires ID.me for verification. I have over 20 locked account. Hit me up let’s deal

Items seized by OIG agents during the execution of a UI fraud search warrant. Agents recovered approximately 30 UI debit cards, over $500,000 in cash, and several notebooks containing personally identifiable information.
Fraudsters also create fake websites to harvest information and take advantage of vulnerabilities: employment, romance sites, and lottery winnings.
On January 24, 2022, Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes Elizabeth Rosenberg provided public remarks at the Better Identity Coalition’s Annual Policy Forum, she stated:

“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.

When some of the states, such as Arizona, recognized that they were being defrauded, they partnered with a digital ID company called ID.me. Almost immediately the fraud ring saw the game was up.

Digital Identity is the Answer
During the Pandemic fraudsters got away with what will likely be known as the most significant heist in history.

"It’s definitely an economic attack on the United States," said FBI Deputy Assistant Director Jay Greenberg, who investigates cases as part of the Justice Department’s Covid fraud task force.

Jeremy Sheridan, who directs the office of investigations at the Secret Service, called it "the largest fraud scheme that I’ve ever encountered."

Now we are seeing signs that fraudsters are building on momentum and income gained during the pandemic to target other sectors:

Tommy Nicholas, co-founder and CEO of Alloy, who helps financial institutions comply with “know-your-customer” regulations, said recently, “fraud is really widespread right now, really bad, and getting worse.” He added, “fraudsters are better funded (flush from defrauding governments over pandemic relief), bolder, and more talented than ever.”

In its recent earnings report, Paypal admitted to finding 4.5 million accounts that “were illegitimately created.”

Mary Ann Miller, from fraud company Proov, suggests “What we’re seeing at PayPal is a systemic issue” that is “related directly to the identity theft and synthetic fraud that we saw during the pandemic.”

In 2021, the FTC reported that consumer identity theft reports related to bank fraud via new accounts were up a dramatic 87% from the previous year.

The NIST 800-63-3 Federal Digital Identity Guidelines are specifically meant to curb these types of challenges.

The United States Financial Crimes Enforcement Director gave a speech on identity in April of this year and made it clear that, “FinCEN encourages financial institutions and service providers to consider specific NIST digital identity standards as they build out their identity proofing and authentication processes.”
Report: ID.me partnered with Arizona Department of Economic Security (DES) to verify unemployment applicants and saved taxpayers billions

- The FTC reported a **2,920% increase** in identity theft related to government benefits from 2019-2020
- The pandemic caused an **enormous spike in unemployment insurance claims** - and associated fraud
- DES saw a **7x** increase in weekly initial Pandemic Unemployment Assistance (PUA) claims from 77k (May 16, 2020) to 570k (Oct 10, 2020)

Sources:
2. Arizona Unemployment Insurance Dashboard

ID.me helped **prevent $75 billion in loss on fraud payments** for Arizona DES

**ID.me driving access**

- Unsupervised Remote enables people to verify online in about 5 minutes
- Supervised Remote offers video chat and supports our commitment to No identity left behind

**ID.me delivering security**

ID.me contributed to a **98.8% decrease in new claims filed.**

"ID.me helped DES save the State of Arizona over **$75 billion** in payouts on fraudulent PUA claims"
**GOAL**

Establish a subject is who they claim to be

**HOW**

Three Different Evidence Pathways to Get to IAL2:

- One Superior / Strong piece of evidence if the issuing body confirmed the claimed identity with two pieces of Superior or Strong evidence and the credential service provider (CSP) checks with the issuer (e.g., the DMV would be the issuing body for driver’s licenses)
- Two Strong pieces of evidence
- One Strong piece of evidence and two Fair pieces of evidence

**OUTCOME**

Increase trust between government and citizens, prevent remote and scalable attacks
ID.me omni-channel solution enables us to reduce fraud while ensuring access and equity; we leverage the best of humans and algorithms working together.

**MOST COMMON -- Typically 85-95%**

- **Online, Self-Serve**

**VIDEO CHAT -- Typically 5-15%**

- Virtual In-Person Proofing via Live Video Chat with an ID.me Trained Call Center Agent

**IN PERSON -- <1%**

- In-Person Proofing at Convenient Locations

If individual can’t get through self-service to verify their identity online → Trusted Referee proofs individual to NIST IAL2 via video chat → Individual goes to a retail location and verifies in person

**NOTE:** Government agencies can offer consumers ability to choose to go direct to human agent

---

1. Percentage of verifications completed via each channel. The reason why there is variation is related to three factors: the level of incentives associated with the service/transaction, the security policy chosen by the government agency, and digital capabilities of the user population.
Portable logins are important because people often need to access more than one government benefit or service.
ID.me provides trusted and portable credentials to verified users for use across public sector agencies.

- **Revenue & Tax**: Tax Filings, Document Access, Pension Funds
- **Workforce Agencies**: Unemployment, Housing & Rental Assistance
- **DMV**: REAL ID Pre-Screening, Fraud Reporting, Renewals & Replacements
- **Healthcare**: Immunization Records, CMS Mandate, MEDICAID Unwinding
- **Licensing**: Business Entity Validation, ex: Medical Marijuana
- **Education**: Progressive Identity Verification, Password Reset, Group Discounts
- **Other**: Disaster Unemployment Assistance, Residency Verification, State Disability Insurance, Paid Family Medical Leave
- **Children & Families**: SNAP/ TANF/ WIC, Child Support
Recommendations

COVID-19 accelerated the need for states to adopt modern identity best practices

- **Embrace Uniform Standards** by enabling NIST 800-63-3, a proven deterrent to fraud
- **Leverage a Network** active across states and the federal government to share intelligence and accountability
- **Maximize Access** for all eligible citizens: include multiple pathways to prove one’s identity with a risk-based policy approach
- **Incentivize Success:** don’t pay for fraud - ensure the real-person is getting through to claim their identity
- **Protect Privacy** and security by putting citizens first and adhere to CCPA
- **Deploy Rapidly** to safeguard your applications and enable immediate access
- **Communicate Often** with data, threat intelligence and more
- **Enable Portability** interoperable credentials allow citizens to reuse the same login - which increases trust
- **Require Accessibility** through multilingual and broader 508-section compliance
Appendix

Pete Eskew
GM, Public Sector
O: 404-502-7497
pete.eskew@id.me
Twitter: @eskewp

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.
At one federal agency’s request, we shifted them to LOA3 based on assessment of low transaction risk (Privacy Act requests); fraudsters attacked the new policy within 6 days. The agency transitioned back to IAL2, and no fraudulent accounts have been identified since.

**KEY TAKEAWAYS**

- **0%** Portion of IAL2 accounts identified as fraudulent
- **9x** Increase in traffic after policy change
- **6 days** Time it took fraudsters to attack updated LOA3 policy
- **89%** Portion of LOA3 accounts identified as fraudulent
- **0** Fraudulent accounts found after return to IAL2
Of the 4.7 million reports filed with the FTC in 2020, **1.4 million claimed identity theft**, more than any other type of complaint.

Roughly **95% of the 160,000** complaints that have been submitted to the DOL hotline mentioned some type of identity fraud. In many cases the complaints were made by individuals who discovered they had been victimized only after they applied for benefits themselves but were denied because someone had already fraudulently obtained benefits using their identity.

Pandemic-related complaints submitted in 2020 to the ITRC: **40%** of these victims were unable to pay their routine monthly bills. Additionally, of those surveyed, **24%** were denied unemployment benefits because someone applied using their information and **21%** had their Economic Impact Payment stolen.
Of the 4.7 million reports filed with the FTC in 2020, **1.4 million claimed identity theft**, more than any other type of complaint.

Younger people reported losing money to fraud more often than older people.

But when people aged 70+ had a loss, the median loss was much higher.

Imposter Scams: About 1 in 5 people lost money.

$1,190 million reported lost.

$850 median lost.

Identity Theft Reports:

- **2920%** for Governments/Benefits Applied For/Received.
- **4%** for Evading the Law.

Age 20-29: $324 median lost.
Age 70-79: $635 median lost.
Age 80+: $1,300 median lost.
ID.me makes identity proofing equity gains permanent by enabling verified users to prove their identity to other agencies simply by logging in.
In comparing partners with and without IAL2+liveness, there is an increased effectiveness in preventing fraud.

Attempted fraud rates were 11-29% higher in states not using IAL2 + Liveness

Date range: 1/28/21-3/8/21

<table>
<thead>
<tr>
<th>Funnel Stage</th>
<th>Federal Agency (LOA3)</th>
<th>State 1 (IAL2 + Liveness)</th>
<th>State 2 (LOA3)</th>
<th>State 3 (LOA3)</th>
<th>State 4 (LOA3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed Possession</td>
<td>139,020</td>
<td>557,022</td>
<td>174,925</td>
<td>75,089</td>
<td>138,988</td>
</tr>
<tr>
<td>Failed Fraud Check</td>
<td>5%</td>
<td>3%</td>
<td>6%</td>
<td>7%</td>
<td>5%</td>
</tr>
<tr>
<td>Failed Identity Resolution</td>
<td>12%</td>
<td>13%</td>
<td>21%</td>
<td>39%</td>
<td>28%</td>
</tr>
<tr>
<td>Total Fraud + No ID Match</td>
<td>17%</td>
<td>16%</td>
<td>27%</td>
<td>46%</td>
<td>33%</td>
</tr>
<tr>
<td>Successful Completed Verification</td>
<td>132,746</td>
<td>333,705</td>
<td>132,439</td>
<td>65,579</td>
<td>103,016</td>
</tr>
</tbody>
</table>
Criminals are increasingly using computer generated 3D masks to attempt to commit identity theft but they have not been successful.
NIST SP 800-63-3 Digital Identity Guidelines defines requirements for federal agencies implementing digital identity services.

2005-2015
Knowledge-based verification (KBV) starts becoming popular on the Internet as an identity proofing technique.

2013
Cybersecurity blogger Brian Krebs concludes seven-month investigation documenting how a crime group, known as the SNSDOB gang, has systematically stolen personal data from Data Broker L, Kroll Background America and Dun & Bradstreet—and then channeled that data to hard-core identity thieves.

2017
- Equifax hack where 145 million American consumers had their personal details stolen
- NIST issues SP 800-63-3 which states KBA cannot be used for identity verification

May 2019
GAO issues report expressing concern that federal agencies are still relying on KBA methods using data from credit agencies despite the fact that NIST no longer endorses it as a verification method.

IAL2
User must submit evidence for identity proofing, remote permitted

AAL2
Multi-factor authentication required, combining forms of authenticators

FAL2
Assertion is signed by SCP and encrypted
Three Types of Fraud: First, Second, or Third Party

First Party Fraud
The actual owner of the identity commits the fraudulent act.

Second Party Fraud
A representative of the owner of the identity commits the fraudulent act e.g. attorney, caretaker, doctor, etc.

Third Party Fraud
A person unrelated to the owner of the identity commits the fraudulent act.