https://insights.id.me/featured-viewpoint/stopping-massive-fraud-and-identity-theft-with-equitable-facial-recognition/?cn-reloaded=1

# Stopping Massive Fraud and Identity Theft with Equitable Facial Recognition

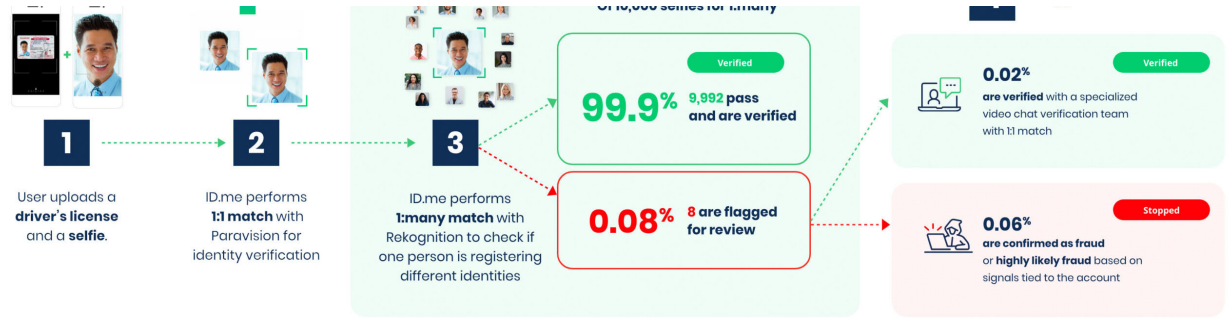
Government benefits fraud is occurring on a massive scale. Sophisticated criminal enterprises have been successfully penetrating government benefits systems with fake identities, resulting in hundreds of billions in losses to state and federal treasuries, victimizing millions of Americans and causing a breach in trust between citizens and their government. The FTC reported identity theft tied to government benefits increased by 2,920% during the pandemic.

To combat this scourge, 30 states as well as federal agencies have looked to ID.me to help verify identities, prevent fraud, and ensure legitimate access to government benefits. ID.me adheres to the mandatory federal guidelines for authentication.

ID.me has prevented hundreds of billions of dollars in government benefits fraud over the last 18 months. The four states that have publicly disclosed the extent of fraud credit ID.me with preventing *$210 billion in fraudulent payments*.

https://insights.id.me/featured-viewpoint/stopping-massive-fraud-and-identity-theft-with-equitable-facial-recognition/?cn-reloaded=1

## How It Works




*Click to expand*

**Selfies are critical to verifying identity and preventing fraud –** We use 1:1 matching for identity verification, and 1: many for fraud detection. We do not share selfies with any government agency unless fraud is detected.

**1:1 Matching is Equitable** – ID.me uses a selfie check — a simple comparison of a selfie to a photo on a government ID — for identity verification. 1:1 face match technology is similar to taking a selfie to unlock a smartphone. This is a mandatory requirement in the federal guidelines for identity verification.

ID.me uses Paravision, a leading facial recognition vendor, for this step. NIST, a federal agency, has published Paravision's results on the NIST website. This testing includes performance across demographic groups. The algorithm is exceptionally accurate with incredibly small variation across demographic groups and skin color.

**Face Liveness Confirmation –** ID.me uses iProov to confirm the selfie is genuine and not a mask or an image. The Department of Homeland Security uses iProov.

**1: Many Catches Serial Attackers –** ID.me uses a "1 to Many" check solely for the purpose of preventing identity theft. This step is designed to see if one person is stealing multiple people's identities. **This process alerts on**

**less than 0.1% of all selfies.** These accounts are moved to a video chat verification session with an expert human agent to finish verification. The threshold for matching is set high enough to detect serial identity thieves while impacting a fraction of 0.1% of legitimate users. For every 10,000 selfies that pass the 1:1 matching step, 9,992 (99.92%) are immediately verified. Only eight (0.08%) of 10,000 are flagged for further review. Six of these are either confirmed as fraud or are highly suspicious with multiple fraud indicators. The other two (0.02%) are verified with white-glove treatment through video chat.

This step is internal to ID.me and does not involve any external or government database. It occurs once during enrollment, and exists to make sure a single attacker is not registering multiple identities. The 1:many check does not block any user from verifying. The 1:many check simply influences the routing, the *pathway,* by which a user can verify. This is no different to how other checks in the self-serve flow – like an international user who lacks a presence in records – would be moved to video chat verification with a Trusted Referee per NIST guidelines.

**What would happen without the selfie check –** ID.me initially deployed an older federal policy known as NIST 800-63-2 LOA3 at state workforce agencies. This policy does not include the selfie confirmation step. When ID.me activated the current NIST 800-63-3 IAL2 with the selfie step, fraud rates fell by 5% to 18% depending on the state. The data clearly shows that fraud would increase by high single to low double digits if the selfie step is removed.

https://insights.id.me/featured-viewpoint/stopping-massive-fraud-and-identity-theft-with-equitable-facial-recognition/?cn-reloaded=1

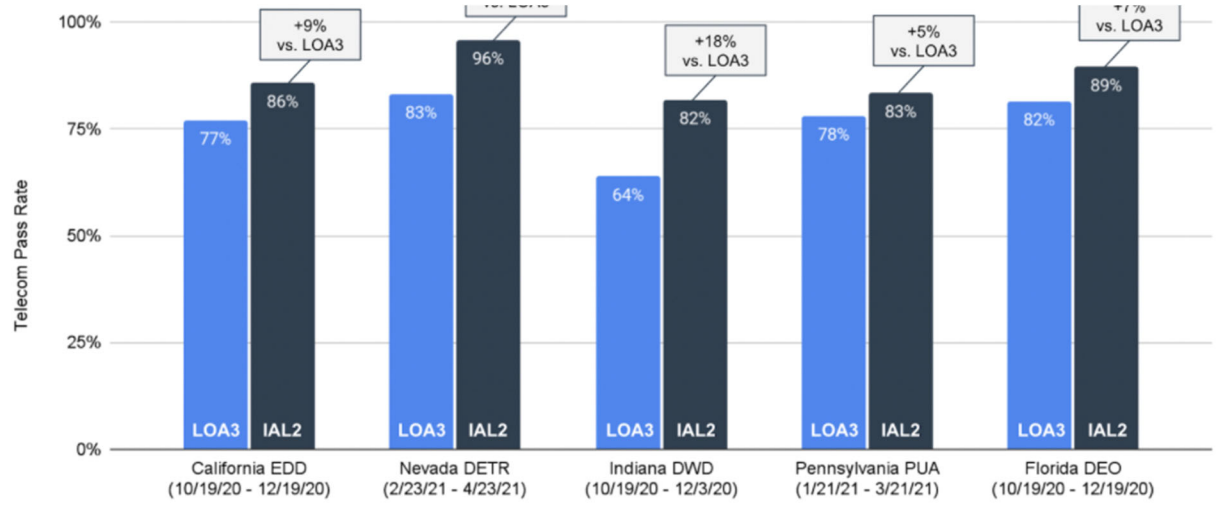



**Figure 1: Reduction in identity theft rates after turning on the selfie step**

A more detailed explanation of ID.me's process will follow in additional posts and our Unemployment After Action Report.

**Why It Matters**

Criminals are lining their pockets with hundreds of billions of taxpayer dollars while hard working Americans become unwitting victims of identity theft, facing delayed payments and diverted funds.

In just one example, Eric Jaklitsch of New Jersey has been indicted with wire fraud and aggravated identity theft. According to court documents, Jaklitsch executed a scheme to defraud the California Employment Development Department (EDD) by filing at least 78 fraudulent unemployment insurance claims. Jaklitsch collected personal identifying information of numerous individuals — including names, birth dates, and Social Security numbers — and used their identities to file fraudulent unemployment insurance claims. He had hundreds of devices and phone numbers registered to the identities of the people he was targeting.

An internal investigation conducted by ID.me identified Jaklitsch as a person conducting a fraud scheme and referred the case to federal law enforcement. The scheme sought over $2,500,000 in unemployment insurance benefits and caused EDD and the United States to incur actual losses exceeding $900,000.

ID.me's investigation provided recourse to victims and the government. Prolific attackers target multiple government programs and private sector organizations. The harm they inflict on each program they target, and on the lives of innocent Americans, cannot be overstated.

One victim of identity theft told NBC News, "It's been a nightmare. My husband and I would have survived better had our house burned to the ground, or if we had been burglarized or robbed at gunpoint. There would have been less hassle, less stress, and less indignation," she said. "It caused the death of our marriage and of everything we've known to be safe and secure. I have no hope or faith of trust in anybody anymore."

Personal devastation like this stands behind massive fraud numbers. ID.me is committed to protecting innocent people and to stopping identity thieves from abusing our social programs.

## Frequently Asked Questions

### Does ID.me disclose your counter-fraud measures to your government partners?

ID.me discloses our use of the 1:many step to our government partners prior to activating it. We have always disclosed this practice along with supporting data to our agency partners.

### Why doesn't ID.me disclose your counter-fraud measures more broadly?

https://insights.id.me/featured-viewpoint/stopping-massive-fraud-and-identity-theft-with-equitable-facial-recognition/?cn-reloaded=1

We avoid publishing identity theft countermeasures to the general public as disclosure can jeopardize the effectiveness of our controls while putting real people in harm's way.

**Does ID.me use external databases or public photos in your 1:many matching?**

No. The 1:many is internal to ID.me and does not involve any external or government database. It occurs once during enrollment, and exists to make sure a single attacker is not registering multiple identities. The selfie is turned into a mathematical representation of a face and then compared against multiple accounts to see if a single person has registered multiple different identities that do not belong to them.

**Do your vendors retain access to photos collected by ID.me?**

1:many selfie data is not stored as a photo with any vendor. Only a mathematical representation of the selfie remains in Amazon Rekognition. Nobody other than ID.me can access this data.

ID.me hosts Paravision's face match algorithm. They do not have access to our photos.

iProov may only retain access to photos tied to fraudulent attacks like masks and deep fakes in order to adapt to criminal activity over time.

**How does ID.me make use of 1:1 vs. 1:many?**

ID.me uses 1:1 face match for identity verification purposes. This is similar to taking a selfie to unlock a smartphone. The 1:many check does not block any user from verifying. The 1:many check simply influences the routing, the pathway, by which a user can verify. This is no different to how other checks in the self-serve flow – like an international user who lacks a presence in records – would be moved to video chat verification with a Trusted Referee per NIST guidelines.

To prevent criminal fraud, ID.me uses a specific "1 to many" check on selfies with respect to government programs targeted by organized crime. This check helps stop prolific identity thieves and members of organized crime from stealing the identities of innocent victims en masse. The 1:many step is

internal to ID.me and does not involve any external or government database or publicly available photos outside of ID.me. This check alerts on fewer than 0.1% of all accounts with a selfie.
On average, for every 10,000 selfies submitted, about 8 people are flagged for review and directed to our Trusted Referee process, 6 of them are either confirmed as attackers committing identity theft or they abandon the flow, and 2 of them are verified after going through video chat verification with a specially trained team.

For example, of 60,158 selfies taken on December 30th, the 1:many check flagged 38 users. 33 of those users had a high probability of being fraudsters who had each stolen the identities of multiple people. Five of the 38 were successfully verified with white glove treatment.

**What vendors do you partner with for facial recognition?**
Paravision (1:1), iProov (Presentation Attack Detection) and Amazon Rekognition (1:many). These vendors are present in our self-serve flow. ID.me has a video chat verification pathway staffed with human agents, Trusted Referees, to assist any user who cannot complete the self-serve flow for any reason.

**Does ID.me maintain a database of faces that map back to original photos and who has access to the database?**
ID.me retains the selfie that was used during the identity verification process. ID.me is the only entity with access to this database. The only time biometric information is shared with a government agency is when there is apparent fraud and identity theft tied to the account associated with the agency.

**How many verification attempts have 1:many been used on? How many ended up fraudulent?**
Through January 25th, 2022 there have been 20,901,406 accounts that have been secured against identity theft with 1:many fraud checks. For every 10,000 identity proofing attempts, on average 8 attempts would have been flagged for review. After a thorough manual fraud review, of those 8

flagged attempts, 2 attempts will result in a successfully verified account. The other 6 attempts have multiple fraud signals, indicating that there is a high likelihood of fraudulent activity.

**Can you explain which faces are being searched exactly? Does the system search across all faces in ID.me's system to look for people with their face on multiple accounts?**

The 1:many check is run once during enrollment per each account to ensure a single attacker is not registering multiple different identities. This check prevents significant identity theft and fraud.

ID.me retains the selfie that was used during the identity verification process. The 1:many search is performed using mathematical representations of the selfie, rather than raw images. Confidence intervals and thresholds are set high enough to catch serial identity thieves committing massive fraud without potentially impacting more than a fraction of 0.1% of all users while stopping remote and scalable attacks. In other words, more than 99.9% of users are not paused for review after completing 1:1 identity verification.

ID.me's database is populated only with images uploaded directly to ID.me from users and not from external sources. The 1:many step is internal to ID.me and does not involve any external or government database or publicly available photos outside of ID.me.

The 1:many check is never used to block a verification attempt. It is implemented solely to prevent identity theft. Accounts flagged for review are moved to video chat for verification with a human agent.

**How do you use 1:many facial recognition?**

It's important to distinguish between how ID.me verifies identity and how they detect fraudulent users/criminals. We utilize 1:1 Face Match to verify a person is who they say they are on government issued documents. This is very similar to the process that many use regularly to unlock their smartphone.

https://insights.id.me/featured-viewpoint/stopping-massive-fraud-and-identity-theft-with-equitable-facial-recognition/?cn-reloaded=1

ID.me uses a specific "1 to Many" check on selfies tied to government programs targeted by organized crime to prevent prolific identity thieves and members of organized crime from stealing the identities of innocent victims en masse. This step is internal to ID.me and does not involve any external or government database. It occurs once during enrollment, and exists to make sure a single attacker is not registering multiple identities. This step is not tied to identity verification. It does not block legitimate users from verifying their identity, nor is it used for any other purpose other than to prevent identity theft.

**Do you connect your facial recognition database to any of your government agency clients?**
No.

**Do you use facial recognition technology during the identity verification process?**
Yes. We utilize 1:1 Face Match during the selfie step to verify a person is who they say they are. We are simply matching their face to the picture on their government issued ID. This is very similar to the process that many use regularly to unlock their smartphone.

The 1:many check does not block any user from verifying. The 1:many check simply influences the routing, the pathway, by which a user can verify. This is no different to how other checks in the self-serve flow – like an international user who lacks a presence in records – would be moved to video chat verification with a Trusted Referee per NIST guidelines.

**Why is it important that you use 1:many in fraud cases, but not 1:many in the verification process? Why not use it for both?**
As we've reported, 1:1 and 1:many Face Match have different uses and accuracy data points. 1:1 Face Match is equivalent to an airport agent comparing your face to the photo on your government ID card. 1:many facial recognition is equivalent to giving your picture to the same agent, putting him on stage at a rock concert, and asking him to pick your face out of the crowd.

https://insights.id.me/featured-viewpoint/stopping-massive-fraud-and-identity-theft-with-equitable-facial-recognition/?cn-reloaded=1

During identity verification, we aim to make the process as seamless as possible while promoting security. Therefore, when an individual gets to the selfie step, we utilize 1:1 Face Match to simply match the individual's face to the picture on their government ID card. This is very similar to the process that many use regularly to unlock their smartphone.

If an individual cannot complete one of the steps, they are moved to a video chat verification agent for assistance. This verification process involves government ID cards and a Zoom style meeting with an ID.me agent. Individuals are able to verify their identity anywhere that has an internet connection rather than having to visit a government agency in-person.

The 1:many check does not block any user from verifying. The 1:many check simply influences the routing, the pathway, by which a user can verify. This is no different to how other checks in the self-serve flow – like an international user who lacks a presence in records – would be moved to video chat verification with a Trusted Referee per NIST guidelines. The 1:many check must alert on multiple different accounts in order to flag an account for review.

Our identity verification and fraud prevention solutions align with the federal standards set forth by the National Institute of Standards and Technology (NIST). NIST is responsible for publishing the federal guidelines for identity verification and authentication. These NIST standards help stop fraud while helping real people conveniently claim they are who they say they are.