The Dark Side of Generative AI

Challenges for Identity Verification

Frances Zelazny

The Future is Here and AI is Challenging Societal Assumptions

Artists embracing cloning and charging royalties for use of their voice

Companies like HourOne allow people to develop avatars for sales, product marketing, etc.

Potential to be a societal equalizer

1000:1 gap in papers on AI resource development v AI safety

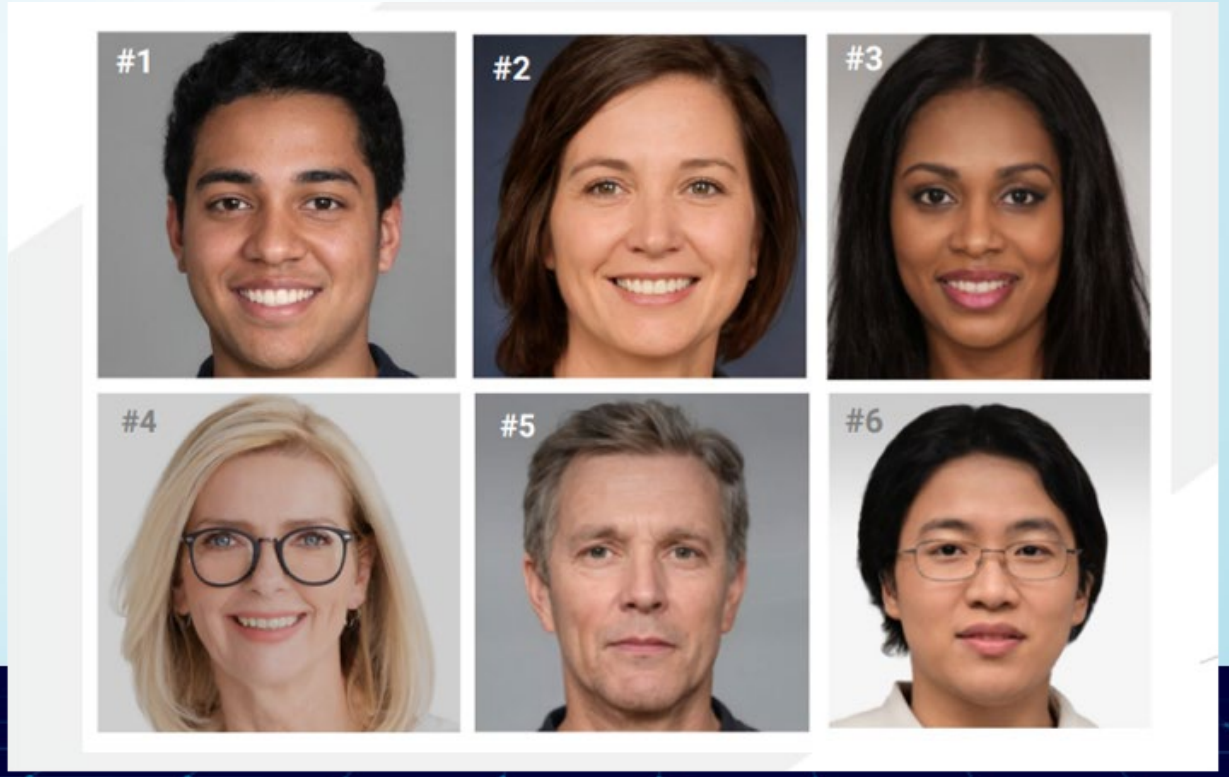
Same AI model that can give every child a biology lesson can give any terrorist a bioweapon lesson

Cyberterrorists selling AI-powered tools for $9.99/mo to enable audio clips that are tied to ransom demands.

Fact or Fiction: AI Generated Fraud

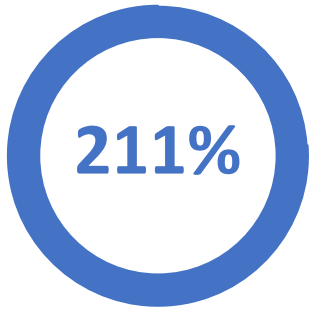
Can you spot the fakes?

Here are six headshots created with generative AI tools. Five are fake. One is real.
Can you figure it out?



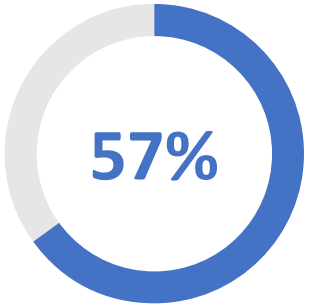
Source: AuthenticID

Even before this really takes off, we are in a fraud crisis.



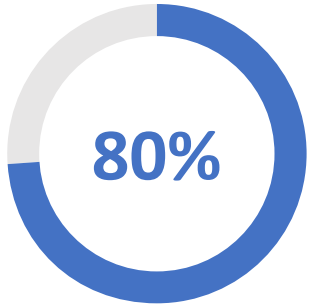
increase in victims who received breach notices

ITRC IDENTITY THEFT RESOURCE CENTER



lost more than $500K in direct fraud

ALLOY



security incidents due to phishing

CSO

in account takeover fraud losses in 2023

AARP

lost in SIM swap attacks in 2023

FBI

The root of all fraud boils down to compromised credentials

Personal data is stored inside central honeypots that are impossible to protect

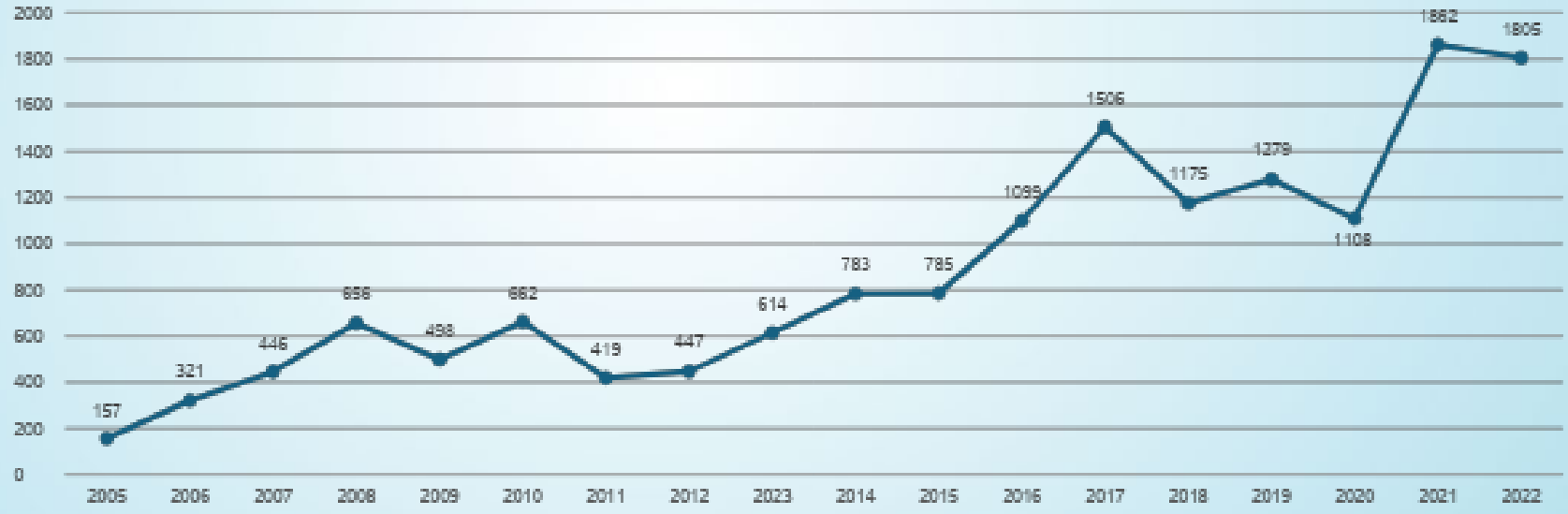
Biometric data collected in account origination is not stored because of privacy concerns

Stolen data is sold on the dark web and used for authentication

Siloed organizational processes create blind spots that attackers exploit

Many enterprises **already collect biometrics** during account origination but **don't store them for fear of data compromises**

Number of Data Compromises



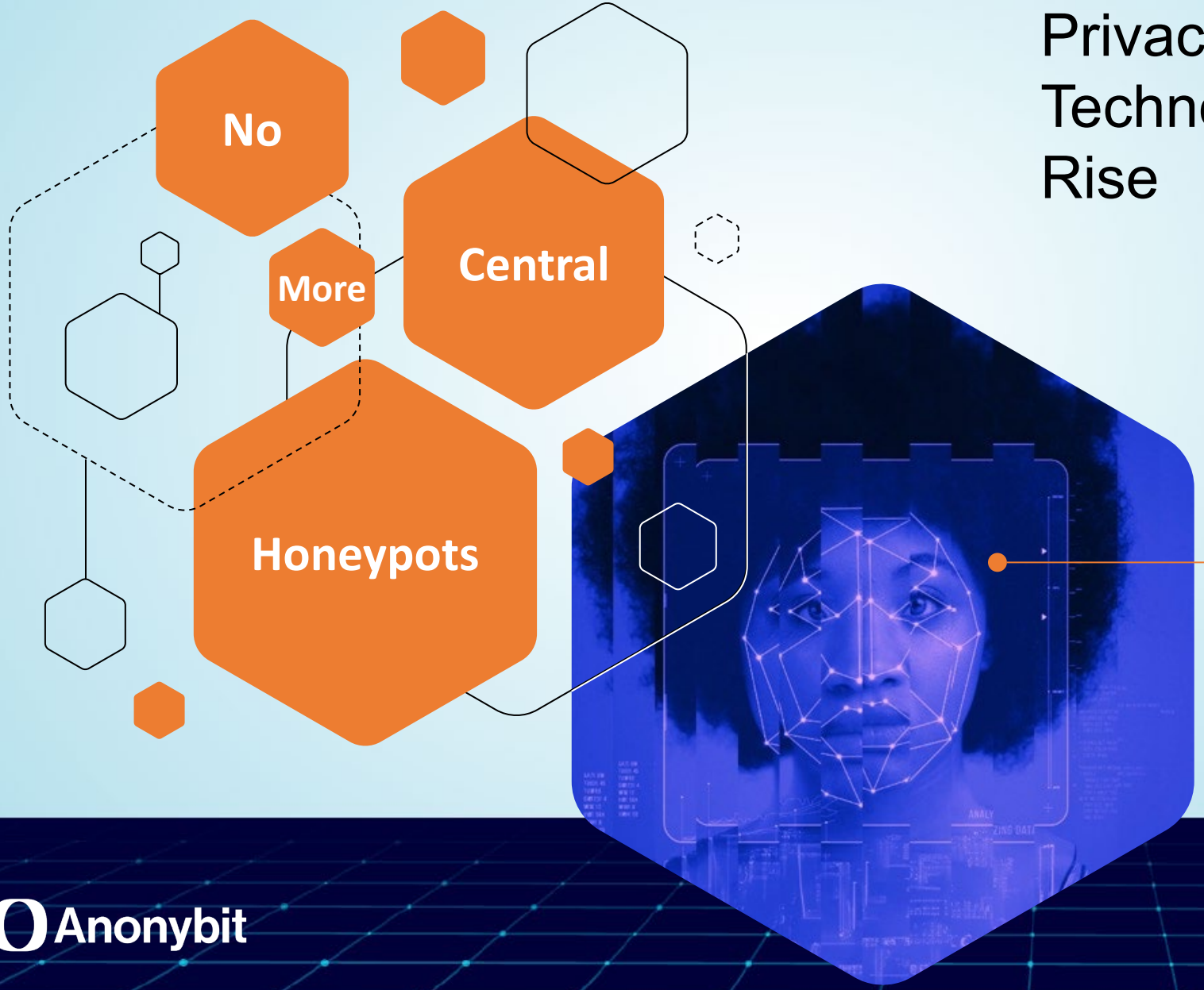
Sources: Statistica 2023, Identity Theft Resource Center, Socure

5 Steps to Combating the Risks of AI Generated Identity Theft

- **Eliminate central honeypots of personal data**
- **Use consistent biometrics across the user journey**
- Use liveness detection
- **Apply injection detection techniques**
- Augment biometric authentication mechanisms with dynamic fraud detection

Anonybit

Privacy-Enhancing Technologies (PETs) on the Rise



Approaches:

Tokenization

Homomorphic Encryption

Secure Multi Party Computation

Zero Knowledge Proofs

Considerations:

Use cases to support (1:1 v 1:N)

Audit and adjudication needs

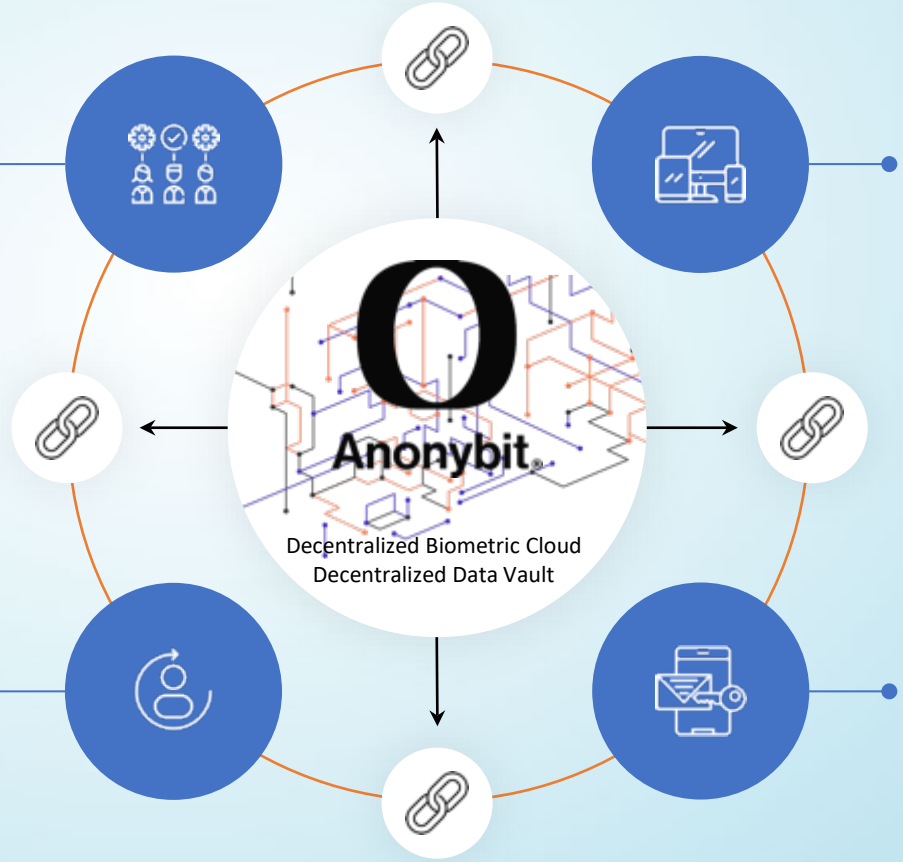
Vendor lock in

Biometric performance

Key/token management

Anonybit's Patented Approach Leverages SMPC and ZKP

The result is a closed **circle of identity** without the gaps that attackers exploit



Digital Onboarding

Ingest biometrics and run a 1:N check to prevent duplicates, blocked identities

Binding

Once uniqueness is established, the biometric is enrolled and bound to a device/token/email or other attribute

Account Recovery

Once the biometric is validated, the token or account can be reset

Authentication

Anonybit is invoked for biometric MFA across service channels/devices with no reliance on KBAs, OTPs, passwords

Combining injection detection with biometric authentication

- Ensure that the verified and authorized user is the one transacting
- Ensure that the data entered by the user is the same as what the bank has received and has not been manipulated

Source: IronVest

Anonybit

THANK YOU

Frances Zelazny
Co-Founder &
CEO
frances@anonybit.
io

The Experience of Identity Verification (IDV)

As it relates to provisioning a Mobile Driver's License Accurately.

David Kelts, 2025-Feb-24

IDENTITY & PAYMENTS SUMMIT
SECURE TECHNOLOGY ALLIANCE | Feb 24-26, 2025

Momentum in Government Online, Digital & Mobile ID

Spots of high activity around the world and beginning to converge into global coverage

2.09 billion
people globally have a Digital Identity or Digital ID

99.4%
of all Swedish Citizens between the ages of **18-67** have a Bank ID that they use for government services

85m of 115m
people in the Philippines have ePhil ID

46%
of the **US population** lives in a state with a live mobile driver's license (**mDL**)

The **European Union** plans for **multiple wallets** and **requires** initial deployments by **2026**

1.3 billion
people covered by Aadhar in India

97%
of organizations experience **challenges** with identity verification using **physical documents** including AI generated fakes

7 States
Australia Fed Initiative deploying mDL & mID in all 7 States starting 2024
NSW: 6M drivers already installed app

Sources:
https://www.bankid.com/en/om-oss/statistic;
https://www.biometricupdate.com/;
https://hub.pingidentity.com/2024-it-pro-survey/ai-and-identity-fraud-protection-take-priority;
Trinisic.ID downloadable Digital ID Adoption Report: https://trinsic.id/adoption-report/
http://www.mdlconnection.com
Matica Technologies Group, S.A.

Who gets an ID or DL?

The universe of people who will register for mDL is larger than the set of people who get a bank account, rent a scooter, take carshare, drive carshare, rent apts.

What will happen if we don’t onboard the right person?

Adoption and trust in Mobile IDs & mDLs depends on the accuracy of onboarding at scale… **global** scale inclusive of everybody

Is remote IDV more accurate than US Postal Service delivery?

Onboarding as a Service

"Ripping IDs"

What could possibly go wrong?

Document Capture & Auth

- Steady hands for Photo of ID?
- High-Res Capture?
- Contrast for Edge-detection?
- Detect specific security features?
- UV and IR Security Features?
- Barcode generated fake data?
- AI generated Fake ID Card?
- Cropping small, obscured, overlaid face from that small captured image of the document

Face Capture for Match

- Duck Lips
- Huge Smiles on Source or Selfie?
- Angled, Distorted Selfies?
- Variable camera resolutions
- Even lighting on facial features?
- Masks, videos, sleeping people?
- AI Generated Synthetic IDs?

- And then the COST!

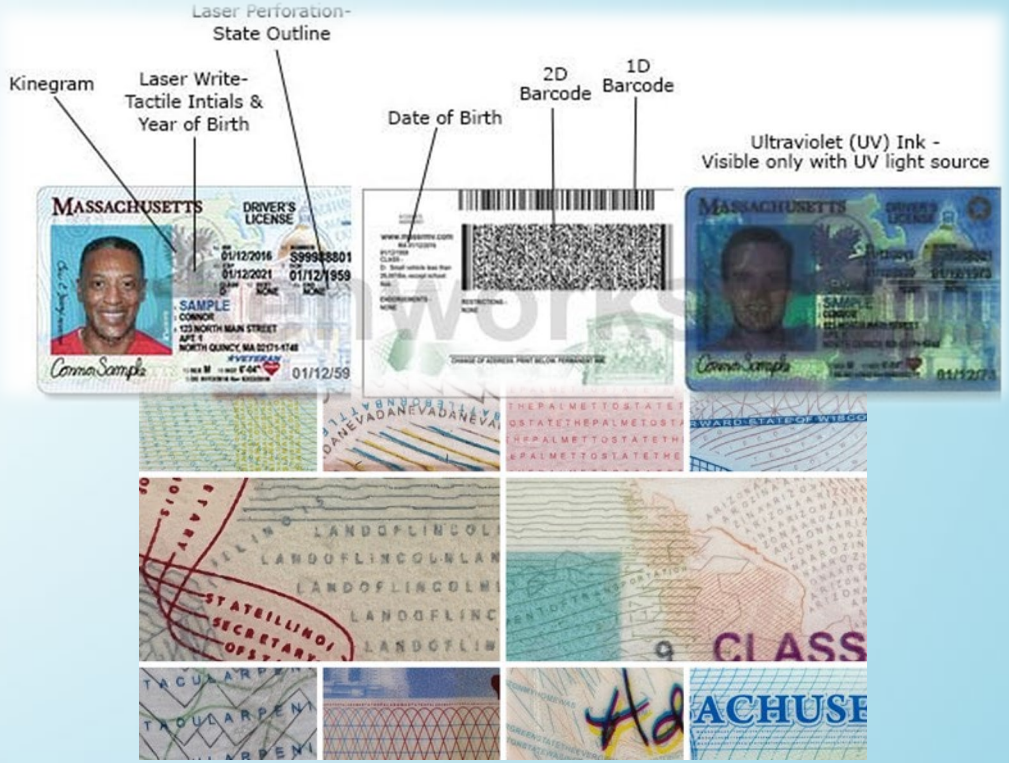
https://medium.com/@dkelts.id/ripping-ids-should-go-the-way-of-cds-49fec9206492

Card Capture & Document Authentication

Can we really expect a dark background? And a non-skewed capture?

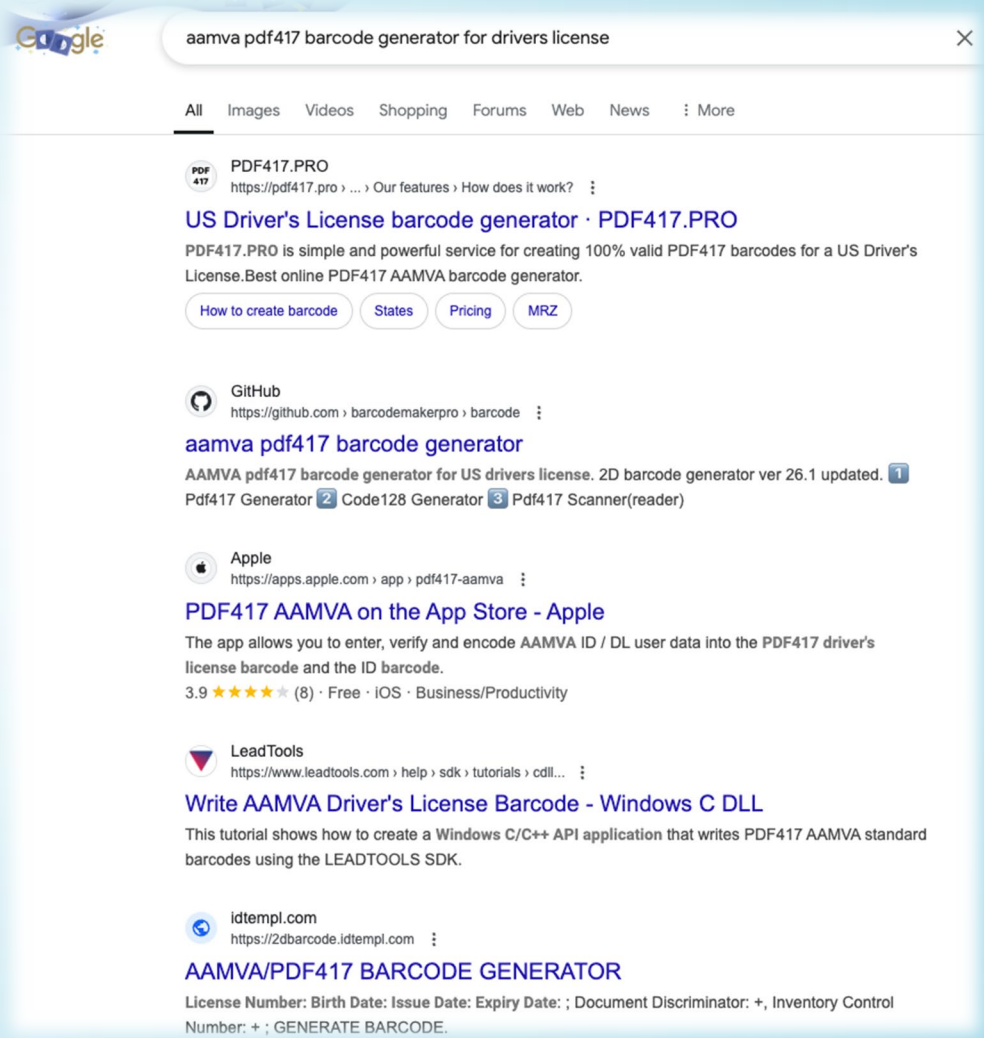
We tend to consider it like this…

How many security features can we detect with the average phone camera?

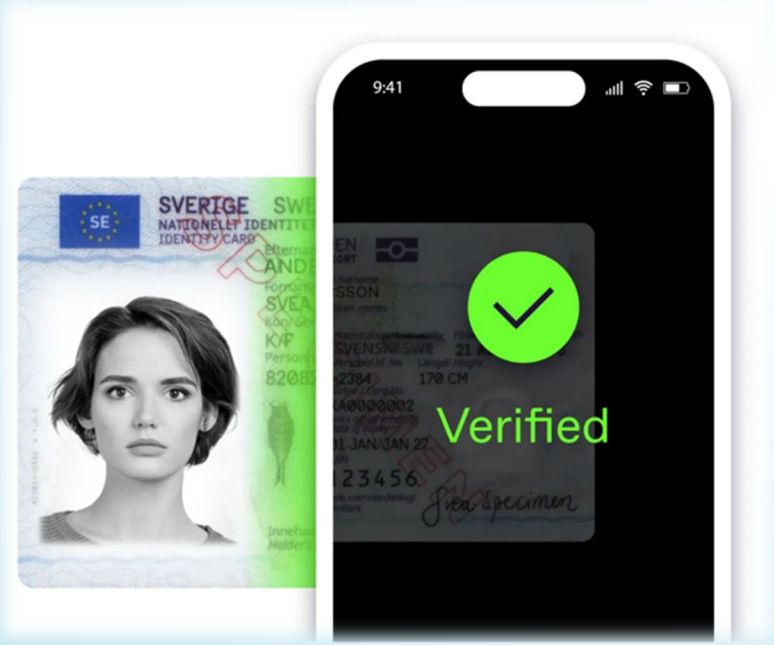


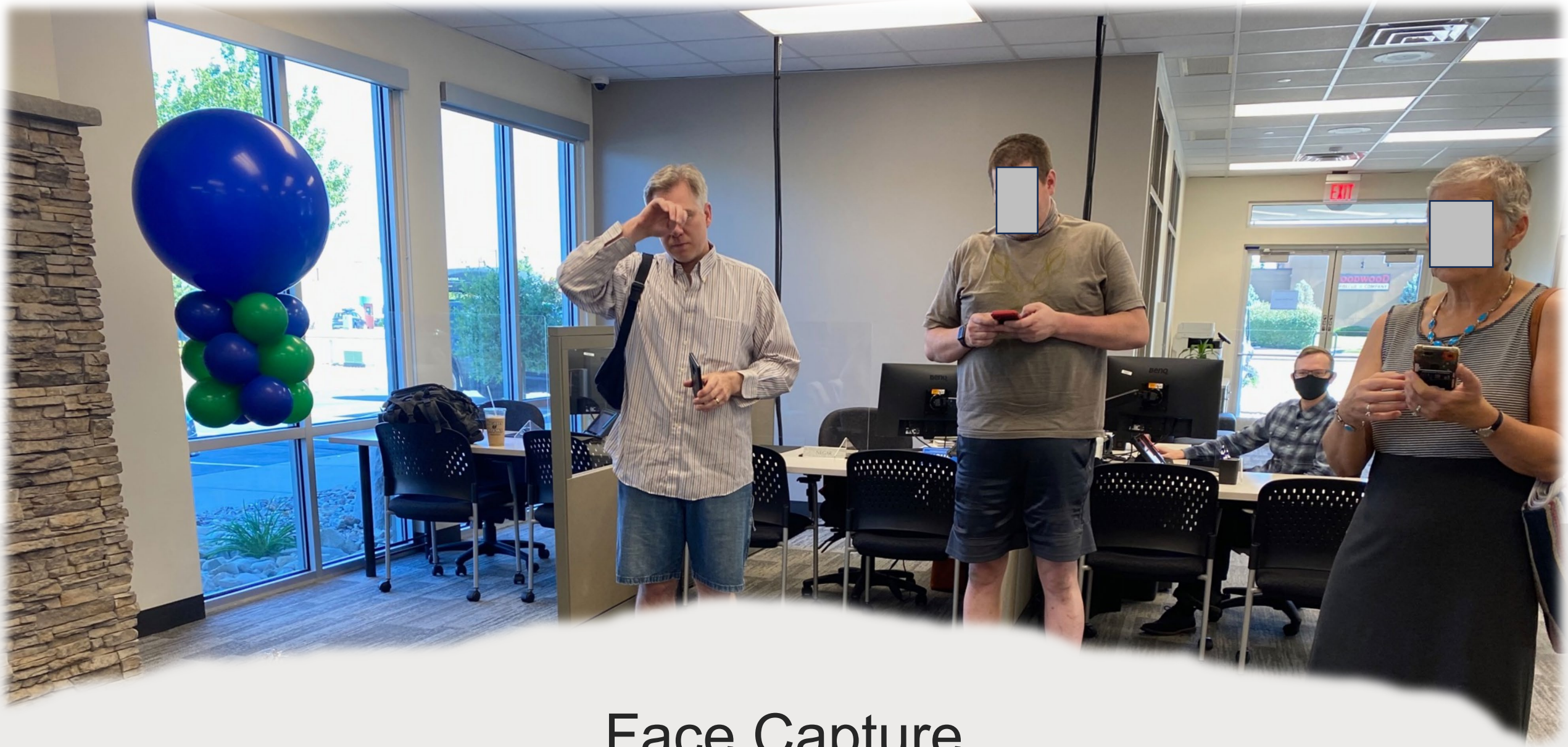
Authenticity of Barcode Data

- Generate any data you want to lay over the existing barcode
  - Front/Back Comparison at the accuracy of OCR from beneath overlays and security line prints
- Every fake ID has a barcode that matches the front of card
  - Barcode anomaly detection as Auth
  - Digital signature in Jurisdiction specific fields (only one state)



Do we have anything more accurate in the USA? Direct read from chip?





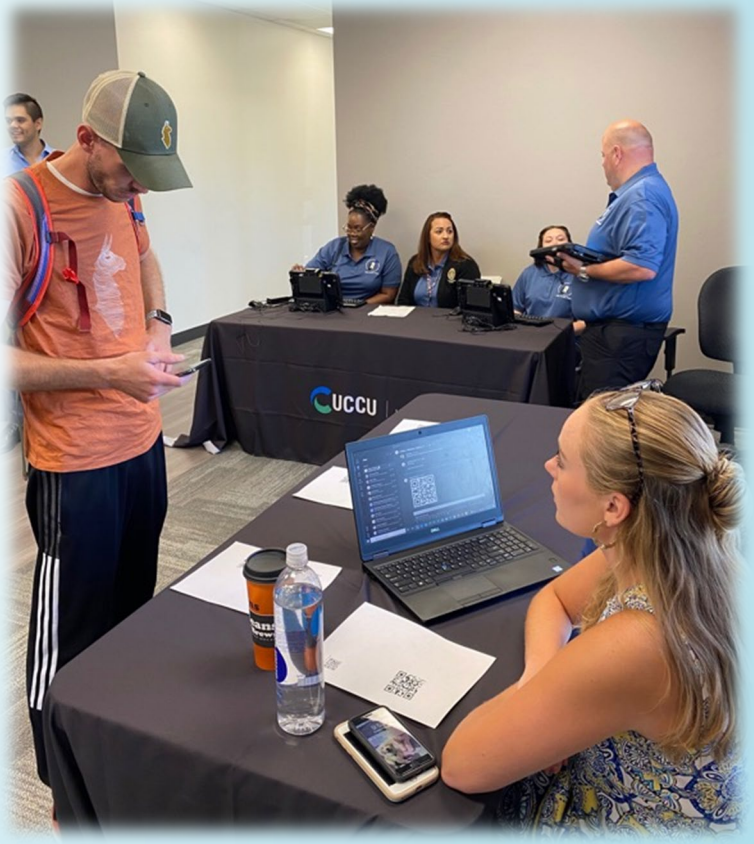
Face Capture

Liveness and Biometric face matching achieving the **expected** accuracy

How do people hold their phone to read instruction text?

- Bifocals and Progressive Lenses
  - Reading distance in lower portion
- Shielding from lit environments
- Comfortable arm positioning

- If we read instructions on a mobile app at all…



Font size defaults for vision or convenience

People set their font sizes LARGE

Are your instructions concise so that somebody could read them?

Are they in written language? Visual-only?

I LOVE MY GIANT PHONE FONT | NOV. 1, 2018

Please Stop Mocking My Phone Font-Size Choices and Join Me in Easy-to-Read Bliss

By Madison Malone Kircher

Turning the font size up on my phone has greatly improved my user experience. Illustration: Intelligencer

I've become conditioned to preemptively declare, "It's not THAT big," anytime somebody looks at my phone screen. It's not that my phone is

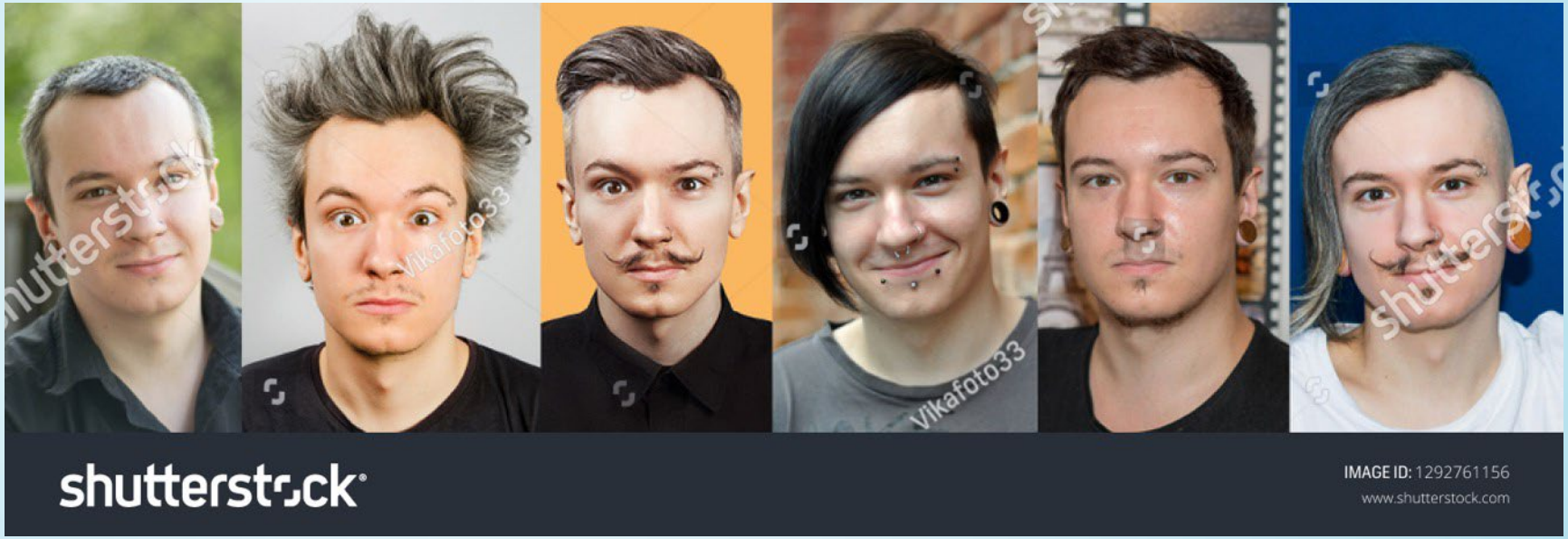
How do people take selfies?

And how do they want their picture to show on their physical card?

Where do people most often register for their Mobile Driver's License?

How is the lighting on both sides of their face?

Social Engineering a Visual Face Match?



This is one way that fraudsters pass as someone else's identity for in-person transactions.

Lens or Barrel Distortion

If people in these photos had different clothes and hair, could you match them visually?

What changes in biometric measurements at different arm lengths?

Cost

If Cardholders expect to pay nothing for their mDL, who is paying for the accuracy that we NEED to build trust in the mDL Ecosystem?