Socure

Hosted by AMERICAN BANKER

Webinar Wednesday, May 1 | 2:00 p.m. ET

Deepfakes and Identity Fraud: Safeguarding Your Business in the Age of Generative AI

David Mattei
Strategic Advisor, Fraud & AML, Datos Insights

Eric Levine
SVP & Head of DocV, Socure

Mike Sisk
Contributing Editor, American Banker

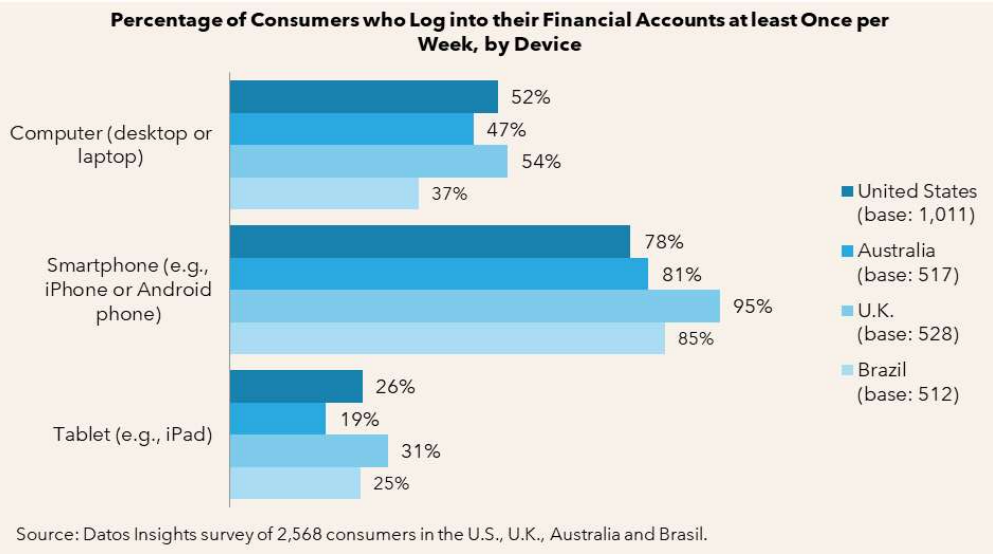
Deepfakes and Identity Fraud

Safeguarding your business in the Age of Generative AI

David Mattei
Strategic Advisor

datos INSIGHTS

Our World is Increasingly Digital



Source: Datos Insights survey of 2,568 consumers in the U.S., U.K., Australia and Brasil.

Source: Datos Insights survey of 2,006 U.S. consumers in Q3 and Q4 2022

Forms of Identity Fraud

ID Manipulation

Real PII data for one person where 1 or 2 pieces of data are altered

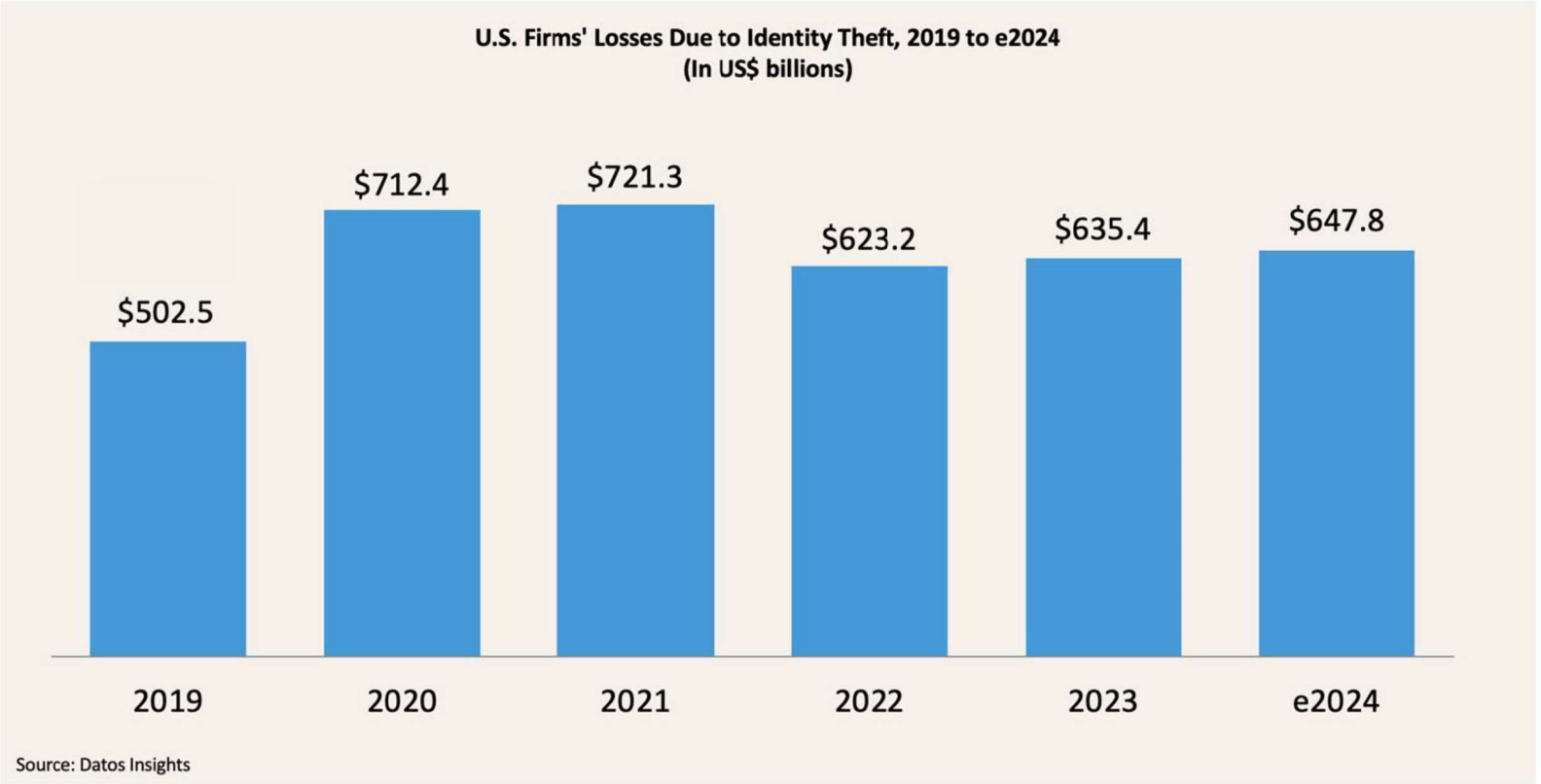
ID Compilation

Real PII data of multiple people are combined to form a new identity

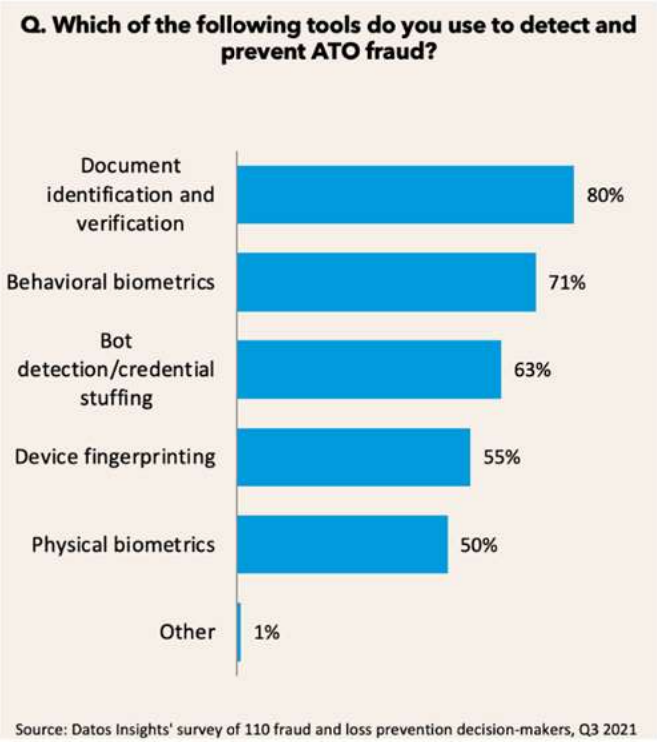
ID Fabrication

Fake PII data used to make an identity

Fraudsters Thrive in the Digital Identity World



Combating Identity Fraud Requires a Multi-Prong Strategy



Deepfakes Are Grabbing Headlines

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

MORGAN MEAKER BUSINESS AUG 9, 2023 7:00 AM

This AI Company Releases Deepfakes Into the Wild. Can It Control Them?

UK unicorn Synthesia offers clients a menu of digital avatars, from suited execs to Santa Claus. But it has struggled to stop them being used to spread misinformation.

Deepfakes will wreak havoc on identity fraud

Deepfake Phishing: The Dangerous New Face Of Cybercrime

Forbes Technology Council

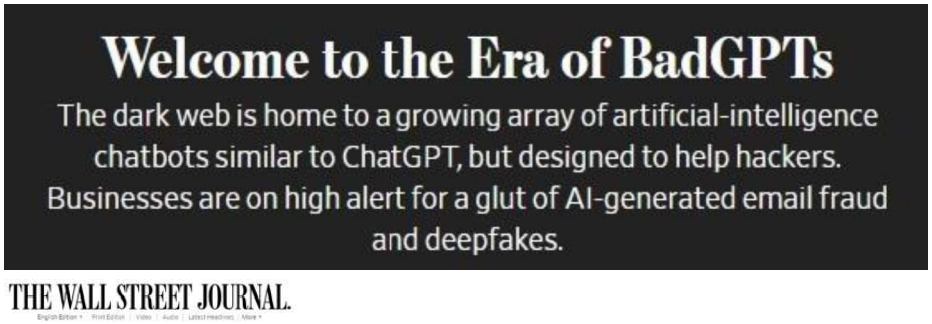
Stu Sjouwerman Forbes Councils Member

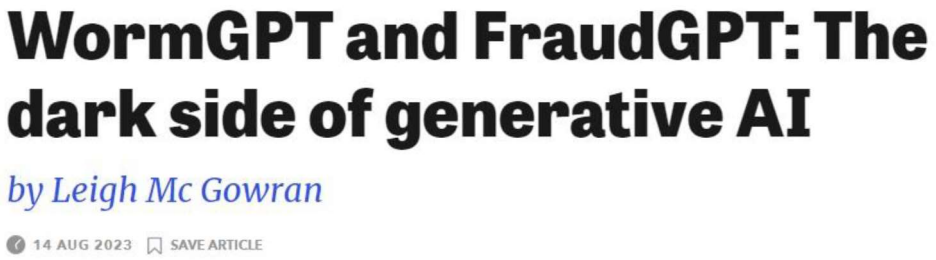
Forbes Technology Council COUNCIL POST

Forms of Deepfakes

- Presentation attacks
  - Pictures / face swapping
  - Videos
  - Masks
  - Voice
- Injection attacks
  - Virtual cameras
  - API/SDK hacks
  - Hijacking payloads in transit

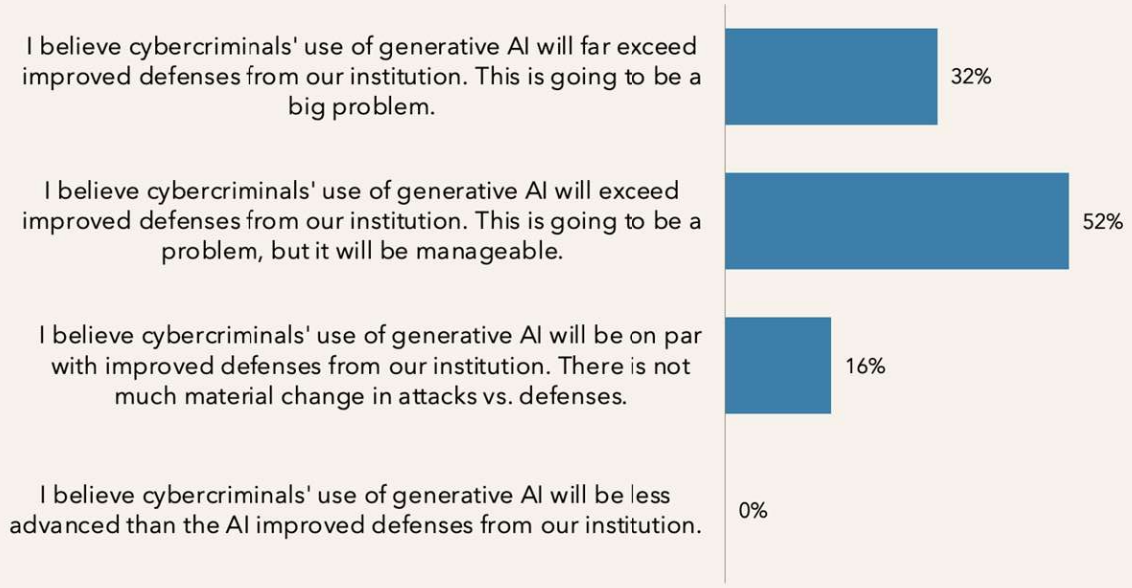
Deepfake tools are cheap and plentiful





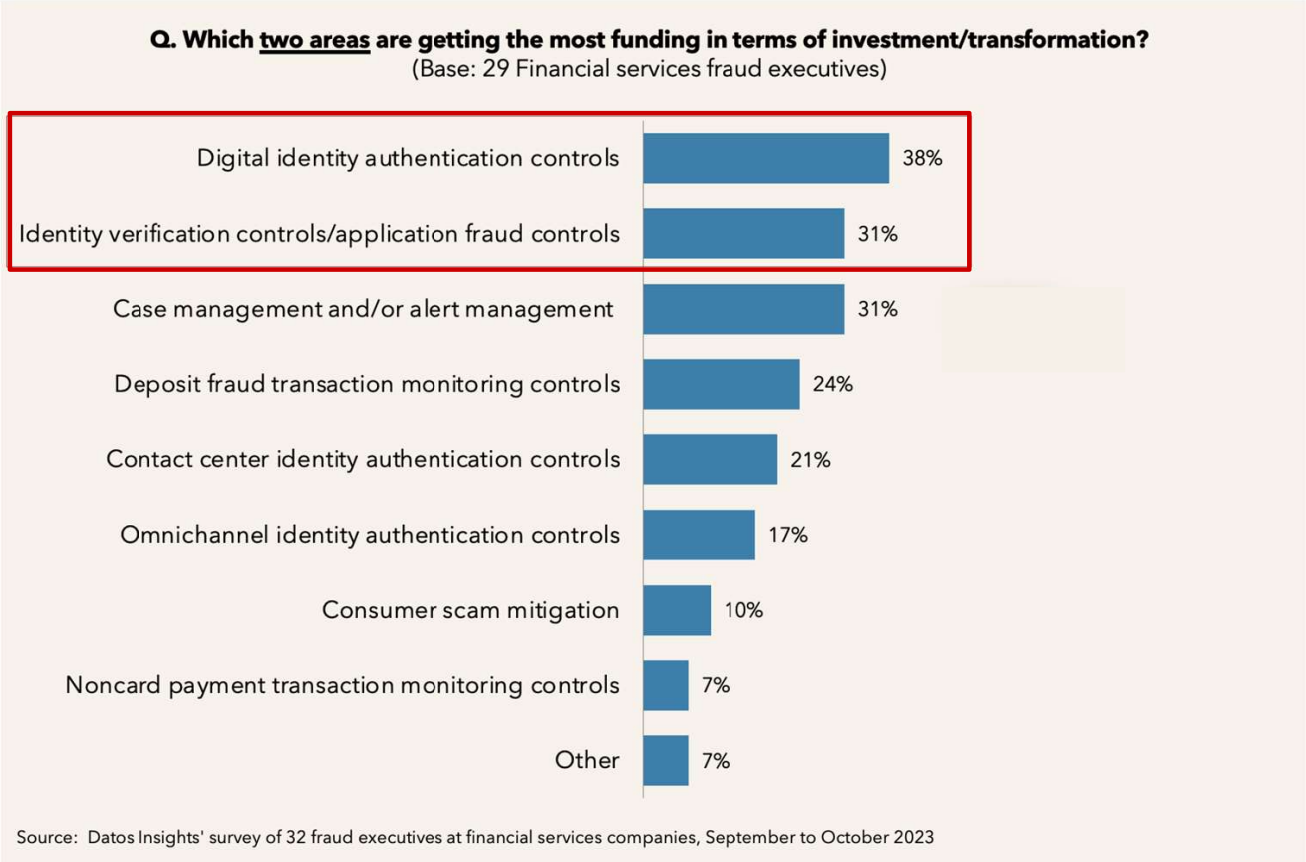
85% of FIs Are Concerned with Fraudsters' Use of GenAI

Q. From a risk perspective, in the next 3 years, how would you predict the impact of generative AI use by cybercriminals in creating attacks, as compared to generative AI's use in defending an institution like yours?
(Base: 25 Financial services fraud exec



Source: Datos Insights' survey of 29 fraud executives at financial services companies, September to October 2023

FI Concerns Are Driving Identity Solution Investments



Source: Datos Insights' survey of 32 fraud executives at financial services companies, September to October 2023

Unmasking Document & Biometric Identity Fraud

Key Terms

Biometrics

Through the unique physical, physiological, or behavioral characteristics of an individual — such as fingerprints, facial features, or voice patterns — biometric identifiers can be used to reliably verify the identity of a specific person

Document Verification

This process verifies a user's government-issued identification document, such as a driver's license or passport, by extracting data from elements like optical character recognition (OCR), machine-readable zones (MRZ), and barcodes.

Selfie Spoofing

Using a prerecorded video or static image to maliciously defeat facial recognition, selfie spoofing attempts to fraudulently access systems or steal identities

Document Presentation Attack

When the user takes a photograph or uses a screenshot image of the ID, rather than getting a live capture of the document; this is also known as "document image-of-image."

Commonly used techniques

63% The most prevalent fraud signal is **document image-of-image — also known as a document presentation attack —** when the user takes a photograph or uses a screenshot image of the ID, rather than getting a live capture of the document.

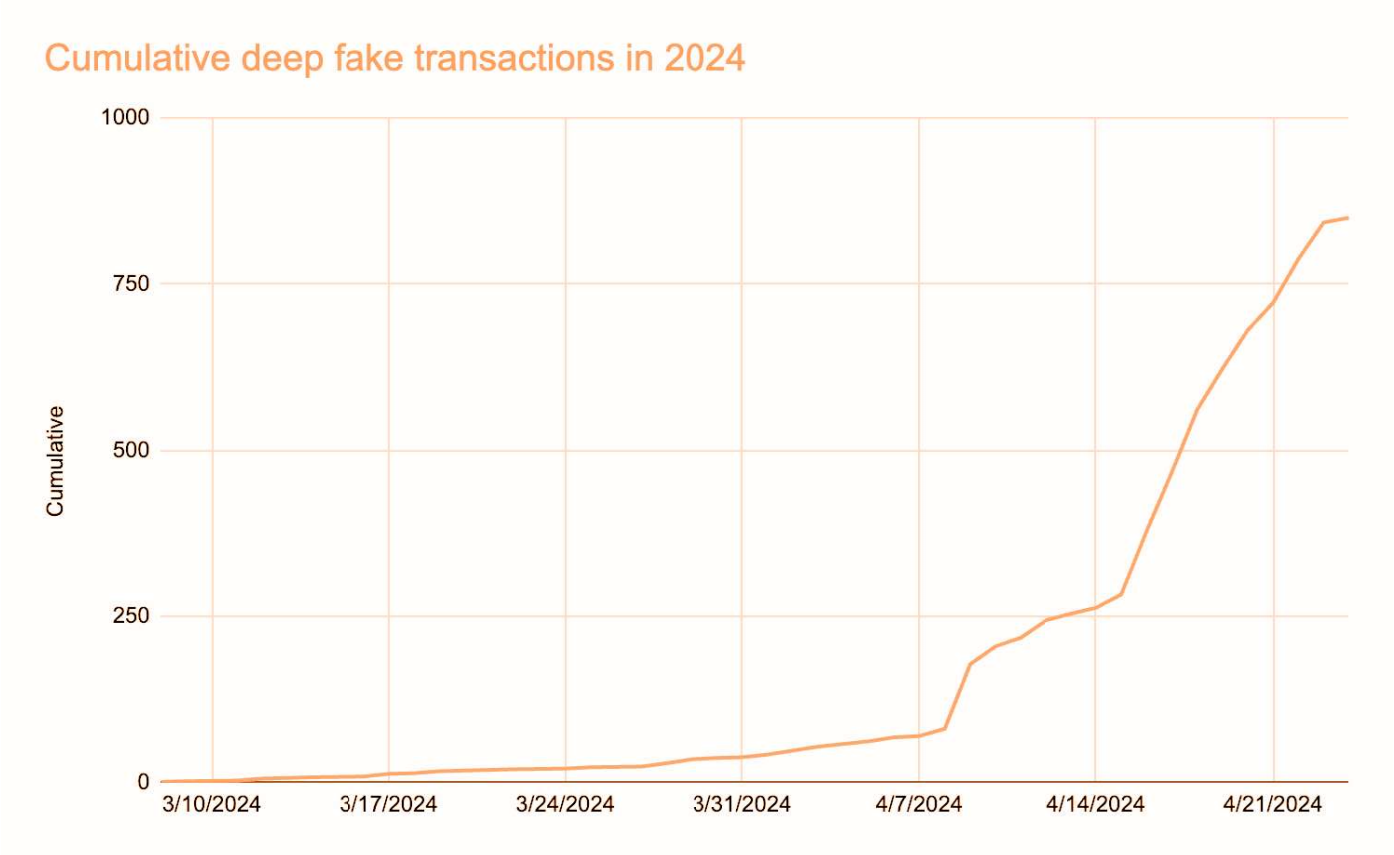
21% We observed a high prevalence of forged IDs containing **document headshot tampering,** where the face on the document has been purposefully manipulated to be inauthentic.

20% **Selfie spoofing** occurs when a user takes a picture of another image rather than simply taking a live selfie of themselves.

11%* **Selfie headshot mismatches** happen when the headshot on the ID does not match the user taking the selfie.

*Note that each percentage represents the percentage of fraudulent verifications where this technique is present. Some verifications may have more than one of these techniques. Consequently, these numbers sum to more than 100%.

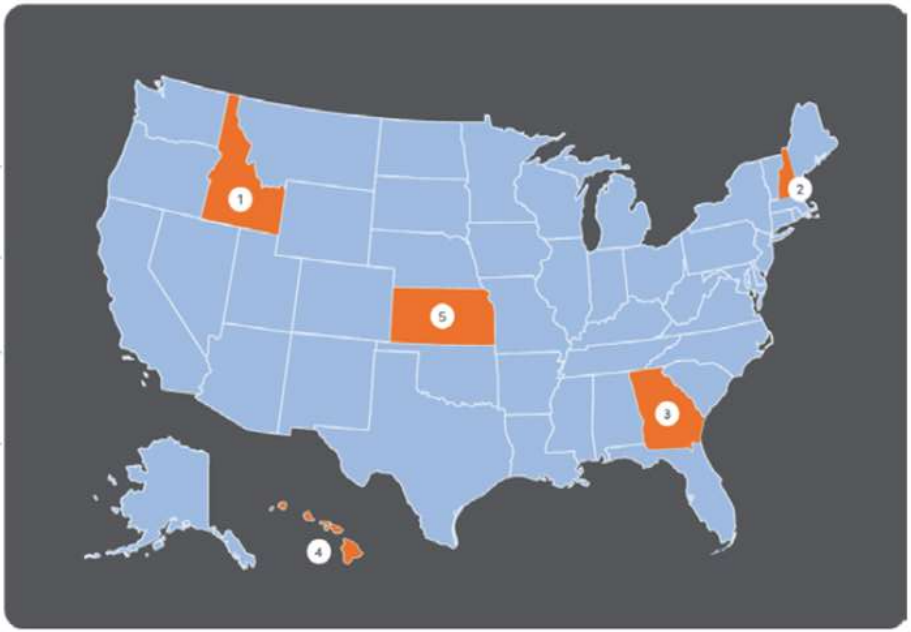
Deep fakes on the rise



Where fake ID’s flourish

- The **top five states with the highest verification reject rates due to the techniques above** include:

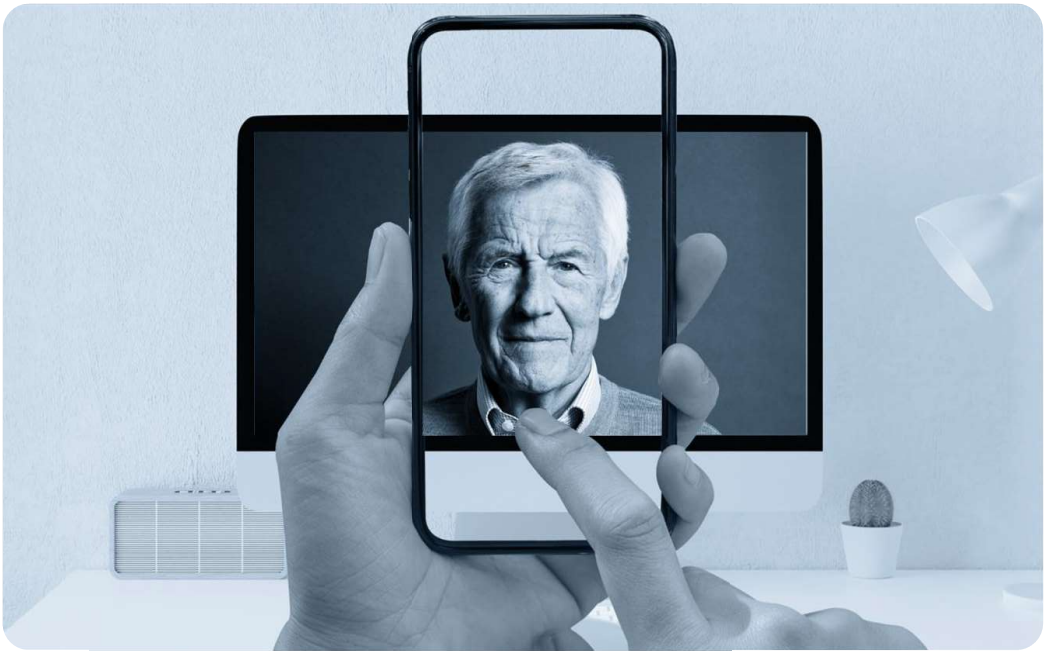
1. Idaho
2. New Hampshire
3. Georgia
4. Hawaii
5. Kansas



The new ID verification paradox

- Younger demographics dominate document verification usage volume, yet fraud plagues those over 50

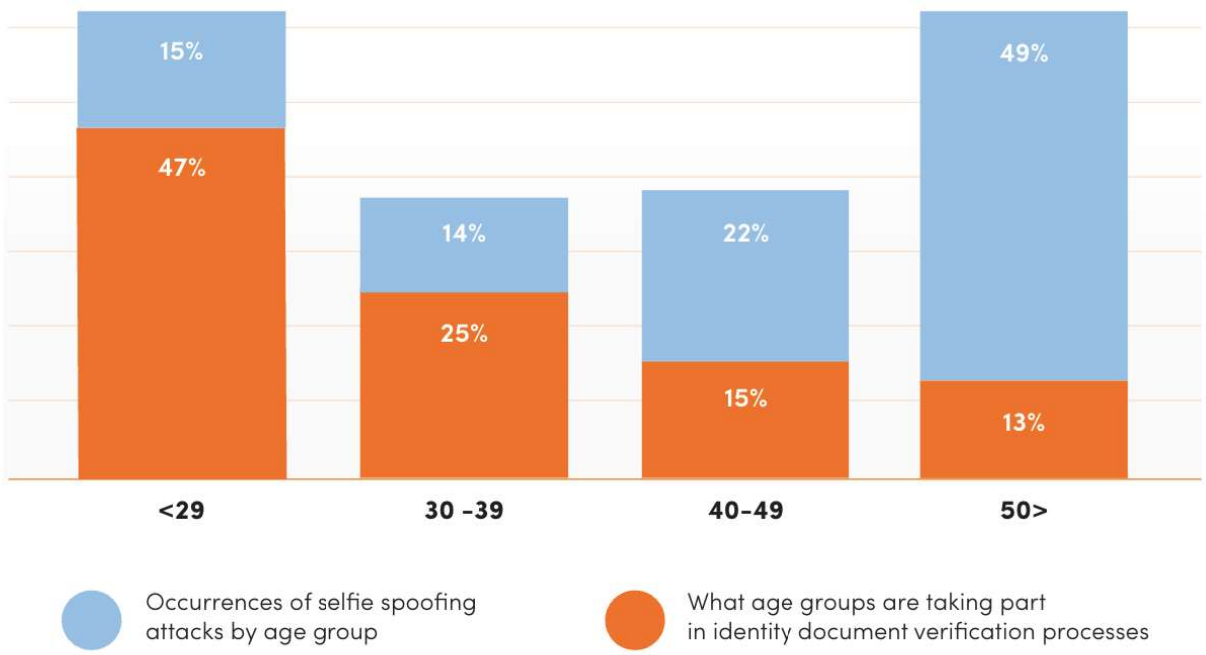
- Nearly half (49%) of all selfie spoofing attacks — where the user takes a picture of another image or a digital screen — target users 50 and above



Socure

The new ID verification paradox

- Younger demographics dominate document verification usage volume, yet fraud plagues those over 50
- Nearly half (49%) of all selfie spoofing attacks — where the user takes a picture of another image or a digital screen — target users 50 and above



Location Deception: When IDs don’t match up

- ⅔ of U.S. ID verifications match device location with ID state; ⅓ show discrepancies.
- 60% increased likelihood of fraud when document & device location don’t match with higher prevalence of multiple fraud signals, non-live documents, and biometric mismatches

The top 5 state IDs with the highest volume of out-of-state verifications are:

1. Florida
2. Texas
3. Georgia
4. California
5. North Carolina

Mismatched Address (the unexpected truth)

- Mismatches between ID state and device location increase fraud risk.
- Over 50% of cases showed discrepancies between user-provided address and ID address, often due to population mobility and outdated IDs.
- Only a 4% higher risk in transactions with matching addresses, suggesting a need for nuanced address verification approaches.

Thank you