REPORT

Socure Identity Risk Insights

Unmasking document and biometric identity fraud: Exposing the deceptions

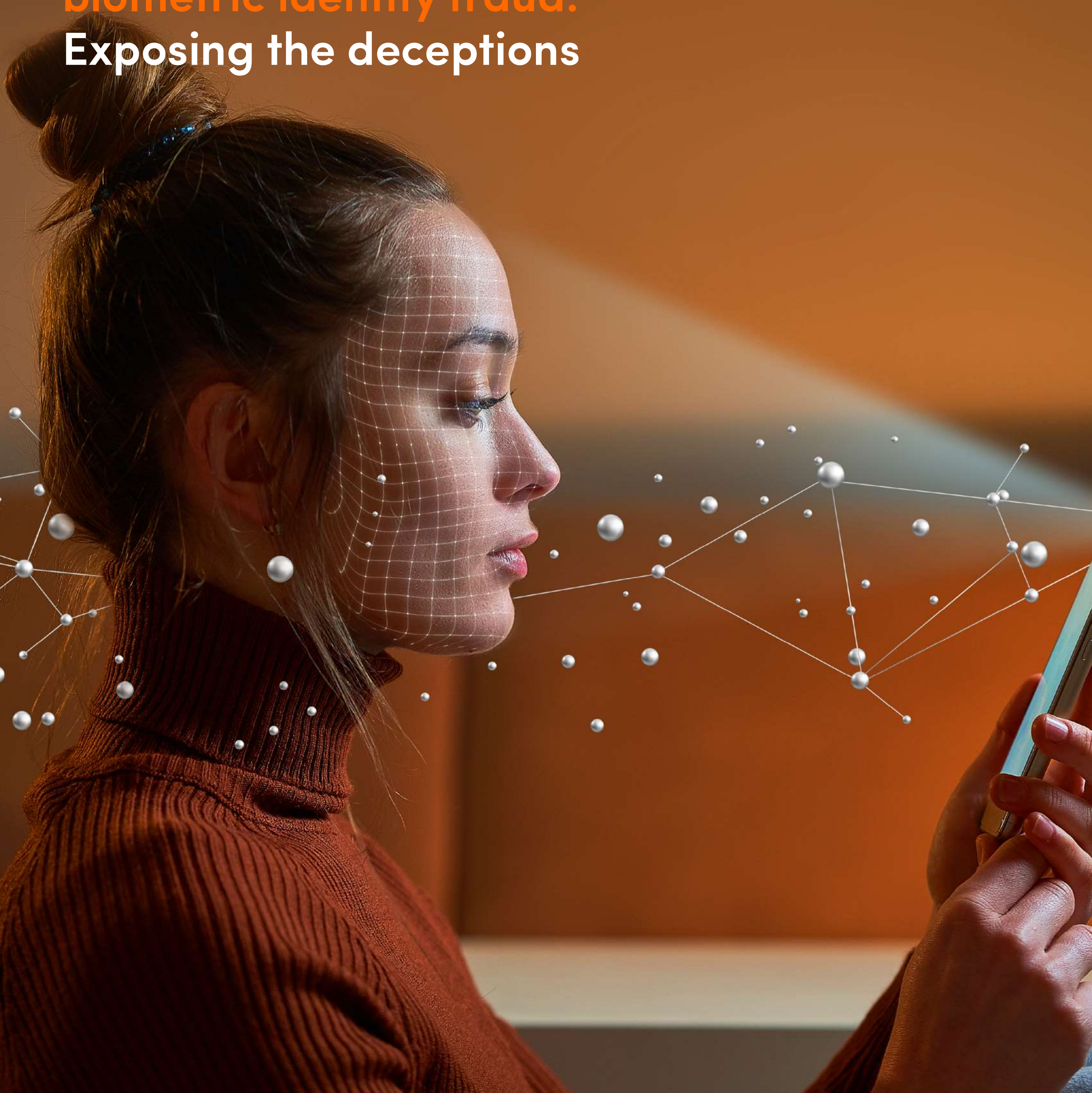


Table of Contents

Battling the next frontier of fraud: Exposing the evolving threats in document verification

Successfully fighting fraud calls for a nuanced approach, one that acknowledges that there are multiple pieces to the puzzle — and not a silver bullet.

One piece of that puzzle is document verification. As a tool on the front lines of fraud prevention, document verification is used in everything from everyday new account opening, to age verification for social media use and two-sided marketplaces.

As generative AI capabilities advance, producing convincing fake IDs and selfies has become easier and more accessible than ever before. These deepfakes are indistinguishable to the human eye and they can deceive traditional verification methods for minimal cost.

Fraudsters now possess the ability to exploit online verification systems at an unprecedented scale.

Financial institutions, once accustomed to tolerating a small number of fraudulent accounts, now face a dramatically amplified threat. A handful of fraudulent accounts is no longer business as usual; vulnerabilities in the verification process could lead to an influx of fraudulent accounts, multiplying the costly impact of fraudsters exponentially.

As technology evolves on both sides, relying solely on traditional document and biometric verification is insufficient.

Instead, an effective solution demands a defense-in-depth strategy — a multi-layered security approach that combines advanced document verification, biometric analysis, and auxiliary signals to create an impenetrable barrier against fraud.

This inaugural fraud report delves into the document fraud techniques we're witnessing at account openings across industries including online gaming, marketplaces, lending and credit cards, real-world attack scenarios, and the path forward.

Key findings

While the findings highlighted throughout this report reflect a variety of fraudulent patterns, we identified some notable trends:

- **According to Socure data from 2023, the overall fraud techniques seen in document and biometric identity verification in the U.S. include the following:**

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.

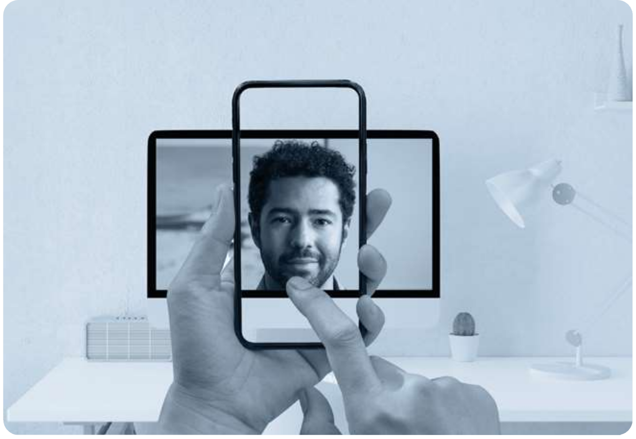
11%*

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

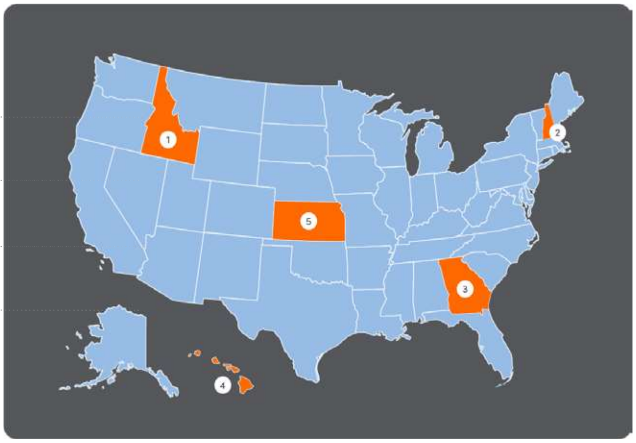
*Note that each percentage represents the percentage of fraudulent verifications where this technique is present. Some verifications may have more than one of these techniques. Consequently, these numbers sum to more than 100%.

- **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.** As this age group makes up less than 13% of the document verification volume Socure evaluated in 2023, we can infer that the older demographic may be targets for identity fraud schemes.

- **When analyzing rejected verification rates state-by-state, Socure observed these most commonly used techniques to commit document-related fraud:**
  - Document image-of-image
  - Selfie-to-headshot mismatch



- 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



- In 67% of observed U.S. ID verifications, the device location corresponds to the state where the ID is from, while about 33% of the time the device location and ID state differ. Though many signals make up a determination of risk, **when the document state and device state match, the fraud rate is about 6%. When the device location and ID state don't match, we see almost twice the rate of fraud at over 10%.**

- **However, address mismatches don't equal greater risk.** Though we may assume that a mismatch between the **address on an ID** and the **address input** on an application may signal fraud, our analysis found these instances **only had a 4% higher rate** of risky verifications. This suggests that address mismatches alone may not be a strong indicator of fraud and should not automatically lead to consumer rejection.

Glossary

Here's how we define a few key terms for this report:

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

Defense-in-depth:
A security approach that includes multiple layers of security controls to protect a system or environment so if one layer of security fails, there are additional layers of defense that can mitigate threats.

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."

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. It also checks for signs of document tampering and ensures the person presenting the ID is physically present.

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

Fakes versus faces:
Fraud by the numbers

In 70% of the fraudulent verifications we evaluated, tampering with the ID document itself was the main fraud signal to be flagged. This is largely due to the document image-of-image signal. While this is a high risk factor, it can often be attributed to good users attempting to go through a document verification process by using a screenshot or copy of their original ID.

Biometric-related fraud made up 30% of all fraudulent captures we saw, which was evenly split between selfie spoofing and impersonations, and a mismatch between the headshot on the ID and the selfie.

We expect to see this trend grow as emerging technologies have made deepfake creation more accessible.

Socure's DocV solution rejects submissions that exceed a specific risk threshold, which increases as we see specific fraud signals, or techniques.

While there are several different types of fraud that can be detected from an ID and a selfie, below are the four most prevalent fraud techniques that Socure saw in 2023:*

**Note: 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%.*

Document image-of-image is when the user takes a photograph or uses a screenshot image of an ID, rather than getting a live capture of the document. This action may not come with fraudulent intent, as good users may attempt to go through a document verification process by using a screenshot or copy of their original ID. Because it's challenging to determine the user's true intent in production, these verifications are often rejected.

Document headshot tampering is when the user purposefully manipulates facial imagery. These are less common but almost always intentional and frequently coordinated. Because manipulation requires greater skill and premeditation, organized fraud rings often use this tactic.

Selfie spoofing occurs when a user takes a picture of an image that is on a computer screen, printed on a piece of paper, or even the actual headshot on the document — rather than simply taking a live picture of themselves.

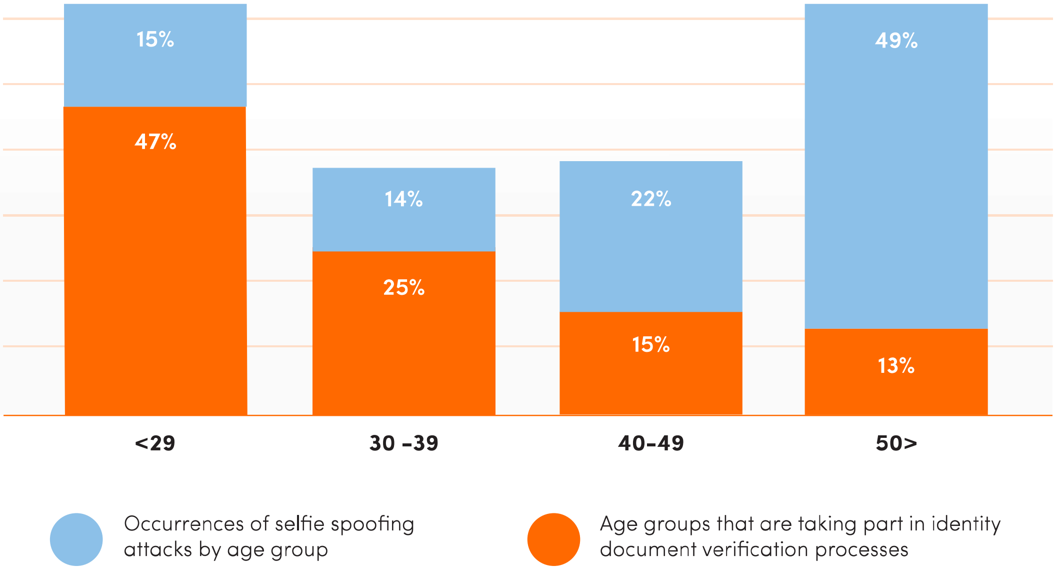
While document image-of-image is not necessarily indicative of fraud, selfie spoofing is more directly correlated with an impersonation attempt through a stolen ID or a completely fake synthetic identity. This can look like a fraudster using images from social media as a "selfie" to go with a recently stolen ID. These stolen images may not necessarily be the same person, just someone who looks similar. This begs the question — could that image you just posted on Instagram be used to help steal other peoples' identities?

Selfie headshot mismatches point to instances of stolen or synthetic identities, as the headshot on the ID itself does not match the user taking the selfie. Selfie headshot mismatch is most likely a one-off attack of someone trying out a stolen ID without making additional modifications.

The new ID verification paradox: Younger demographics dominate document verification usage volume, yet fraud victimizes those over 50

Organizations rely on accurate and rapid document verification across numerous use cases, from expediting rental car pickups to vetting identities for rideshare onboarding. Any lapse in precision or efficiency can have severe consequences.

Interestingly, the user demographics participating in these critical verification processes skew heavily toward younger age groups. In 2023, those under 40 comprised 72% of all document verification activity that we processed — 47% were under 30 years old, and 25% were in the 30-39 age group.



49%

Nearly half (49%) of all selfie spoofing attacks target users in the age 50 and above population.

Often, institutions rely on passive verification methods such as verifying personal identifiable information (PII). If applicants can be verified with that alone, they would not be sent to document or biometric verification. Older, more established users likely have an easier time being approved through passive checks because of their longer credit history.

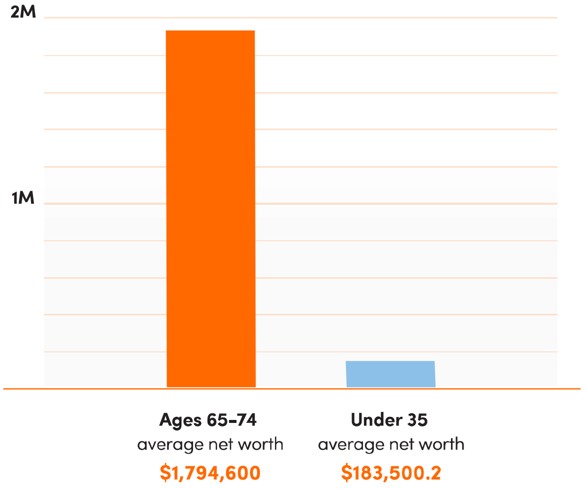
In 2023, Socure saw document verification volumes drop substantially for older groups — the 40-49 group took part in just 15% of volumes, and the 50+ just 13%.

When it comes to impersonation targets, we saw the opposite trend. Nearly half (49%) of all selfie spoofing attacks target users in the age 50 and above population.

As this age group makes up less than 13% of the document verification volume Socure evaluated, we believe older demographics are likely targets for both identity and synthetic identity fraud schemes.

Another factor that makes this age group appealing to fraudsters? According to The Federal Reserve's 2023 Survey of Consumer Finances, the average net worth of individuals peaks between ages 65-74 at $1,794,600, while the lowest net worth individuals are typically under age 35 with an average of $183,500.[2] Identity thieves often target older populations because they can more easily exploit those individuals' personal information to carry out financial crimes — often with a higher reward.

Why 50+ age group appeals to fraudsters



Where fake IDs flourish: Mapping fraud tactics across the U.S.

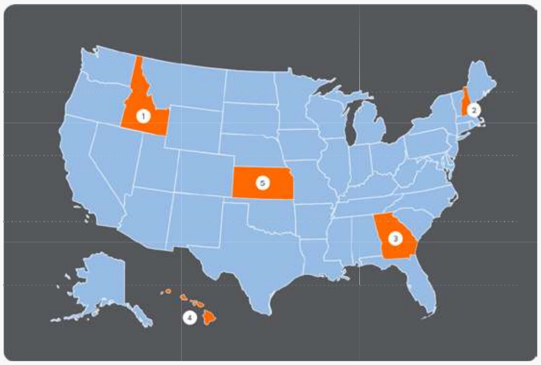
When analyzing rejected verification rates state-by-state, Socure observed that the following techniques were most commonly used to commit document-related fraud:

In the verifications rejected by Socure, document image-of-image was most prevalent because this signal includes not only presentation attacks with fraudulent intent, but also non-fraud where users attempt to reuse prior photos of their IDs.

With the understanding in mind of which techniques fraudsters are using to commit document fraud, where then is this fraud occurring most often? To include other potential avenues of fraudulent attacks on documents, we can add selfie image-of-image and barcode/MRZ mismatches to the list of fraud reasons when evaluating reject rates. These signals occur only a small fraction of the amount that the top fraud signals do, but lend additional breadth to the rejected verifications for our viewing.

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



From this, we can gather that fraudsters may target less commonly seen documents to spoof or use alongside a biometric spoof, perhaps due to a perception (or reality) that **documents from highly populous states like Texas, Florida or California may have increased security measures.**

Location, location, deception:
When IDs don't match up

Beyond looking at the how of attempted fraudulent verifications by state, we also analyzed from where verifications originated.

When the document state and device state **match,** the fraud rate is **about 6%**

When the document state and device state **don't match,** the fraud rate is **over 10%**

In 67% of observed U.S. ID verifications, the device location corresponded to the state where the ID is from, while about 33% of the time the device location and ID state differed.

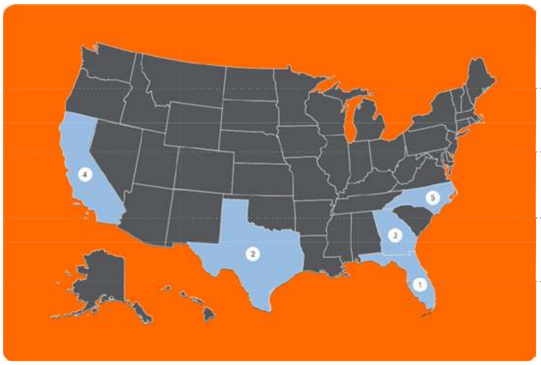
During the timeframe of this report, the overall fraud rate for all DocV verifications was 7%. When the document state and device state match, the fraud rate is about 6%. When the device state and ID state don't match, we see almost twice the rate of fraud at over 10%.

We believe there are several reasons for this:

- Fraudsters may deliberately target identity documents from states with weaker security features, as these are the easiest to forge or misuse, even if they don't match the criminal's actual place of residence.
- If criminals intend to use this document for any in-person business, they might deliberately choose one from another state because they think it's less likely to get caught.
- For certain industries, like online gaming, people may cross state lines to bypass state- or region-level bans on certain apps.

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



The fraud rate almost doubles for out-of-state transactions (10%) relative to in-state transactions (6%), as bad actors attempt to spoof systems and manual reviewers.

Specifically, for out-of-state verifications, we see a higher prevalence of:

2.5x more often

More than one fraud signal at once, such as document image-of-image, headshot tampering, spoofed selfie, selfie image-of-image, or document front/back mismatch.

1.5x more often

Non-live documents, such as using a screenshot of a document rather than a live capture.

1.5x more often

Biometric mismatches, or when a selfie doesn't match the image on an ID.

While out-of-state verifications alone are not a strong predictor of fraud, **they do represent one of many low-precision fraud signals that can be used in a defense-in-depth approach to identity verification** including a broader view of the identity risk by also analyzing PII, barcode data, device and behavioral intelligence, geolocation, and biometric signals.

For out-of-state verifications, multi-risk fraud cases where there is more than one fraud signal, occur nearly

2.5X more often.

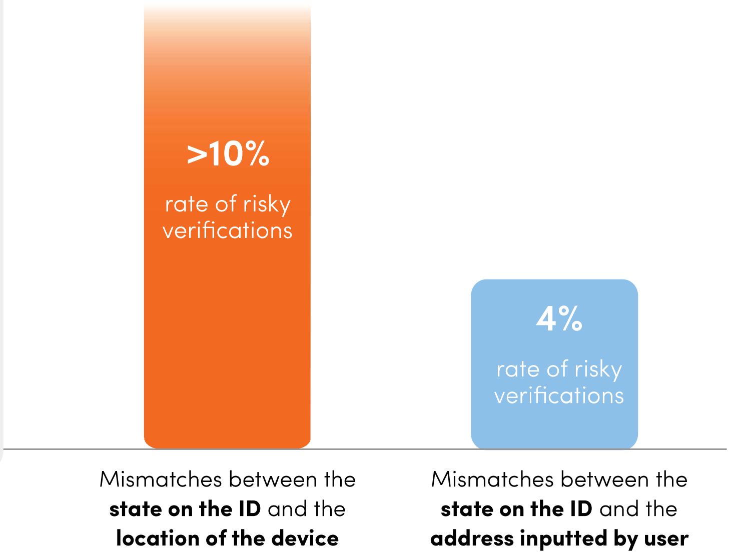
The unexpected truth: Mismatched addresses, lower fraud risk

Our analysis found that mismatches between the state on the ID and the location of the device were indeed associated with elevated fraud risk. **However, the data showed the opposite pattern when comparing the input address to the one on the ID.**

Socure observed that the address provided by a user did not match the ID's address in more than 50% of cases. We attribute this high rate of address discrepancies to the mobility of the modern population, as well as the common practice of many states not issuing updated IDs when someone moves.

Our analysis **showed only a 4% higher rate of risky verifications when the inputted address did not match the address on the ID.** This suggests that address mismatches are not necessarily indicative of higher fraud risk, and may in fact be more common occurrences that do not automatically warrant rejection of a consumer. In these cases, a more nuanced, contextual approach to address verification is warranted, rather than defaulting to rejection based on this single data point.

Socure observed that the address provided by a user did not match the ID's address in **more than 50% of cases.**



The evolving battleground: Staying ahead of document and biometric fraud

97%

Socure's DocV achieves 97% acceptance rates of good customers on the first try vs. the industry standard of 80%

In the rapidly evolving landscape of document fraud, one thing is clear: organizations must adopt a multi-layered defense system to effectively combat sophisticated threats.

Relying solely on traditional document and biometric verification methods is no longer sufficient, as fraudsters leverage advanced technologies like generative AI to produce convincing fake IDs and selfies.

Addressing the complexities of document fraud

Socure is fighting back against emerging fraud threats with its DocV solution. Powered by a combination of computer vision, machine learning, and generative AI technology, DocV creates a holistic view of identity, bringing a defense-in-depth approach to accurately detect fraud including deep fakes, visually indistinguishable fake IDs, or increasingly sophisticated attempts at spoofing ID verification systems.

DocV uses intelligent, automated technology to rapidly analyze hundreds of data points and fraud signals — from biometric matching to barcode forensics — delivering exceptional speed and accuracy that far surpasses human-based processes. By guiding users through an optimal image capture experience and continuously learning from vast datasets, DocV can detect even the most advanced ID forgeries, tampering attempts, and spoofing attacks.

DocV seamlessly integrates with Socure's industry-leading identity verification platform, providing a holistic solution that utilizes device risk/ownership, phone ownership, PII verification, fraud modeling, and hundreds of security and authentication checks, all in a single decision. This multi-faceted approach ensures a robust and comprehensive fraud prevention strategy that goes well beyond just document and biometric verification, enabling organizations to stay ahead of today's evolving threats.

Appendix: Methodology

Data source and metadata

Visualizations and insights found in the report were derived from Socure's production data in 2023. Metadata used for analysis included those models' scores, flags based on model scores, reason/rule codes generated from flags, and finally decisions on whether to accept each transaction based on the derived flags. In addition, verifications themselves provided demographic information such as age, sex, document state and device state obtained from verifications' associated documents and device data. This information allowed for insights into specific fraud vectors, breakdowns of fraud by available demographic groups, prevalent fraud vectors in industry verticals such as online gaming, marketplaces, lenders, credit card, and more. The production data included new account opening, as well as conducting other verifications throughout the customer lifecycle.

Data manipulation

The dataset described above was amassed via a query to a Socure database containing transaction metadata, with additional manipulations such as estimating individuals' age via the transaction date and document date of birth, grouping certain reason codes to demarcate distinct risk vectors, and obtaining more granular information on the risk level of a transaction (was the transaction rejected due to presence of risk vectors indicating a fraud attack, or due to the presence of vectors that simply rendered an accept decision too risky?).

Analysis approach

Analysis was exploratory in nature and as such was largely iterative; first passes at the data showed high-level trends in production traffic, such as transaction volume over time, overall demographic composition, and overall fraud/risk signal composition. Following from questions and corresponding hypotheses, further iterations delved into specifics such as demographic compositions of individual fraud vectors, verifications with mismatched document and device states, or fraud vector appearance rates over time in a particular industry vertical. Included in this report are the visualizations that led to and provided the most salient insight both for initial hypotheses at the start of the report and for questions that arose over the course of this process.

Additional resources

See DocV in action

BOOK A DEMO

Learn best practices for implementing biometric verification

DOWNLOAD WHITE PAPER

Citations

Changes in U.S. family finances from 2019 to 2022. Federal Reserve Board Publication. (2023, October). https://www.federalreserve.gov/publications/files/scf23.pdf

About Socure

Socure is the leading platform for digital identity verification and trust. Its predictive analytics platform applies artificial intelligence and machine learning techniques with trusted online/offline data intelligence from physical government-issued documents as well as email, phone, address, IP, device, velocity, date of birth, SSN, and the broader internet to verify identities in real time. The company has more than 2,300 customers across the financial services, government, gaming, healthcare, telecom, and e-commerce industries, including four of the top five banks, 13 of the top 15 card issuers, the top three MSBs, the top payroll provider, the top credit bureau, the top online gaming operator, the top Buy Now, Pay Later (BNPL) providers, and over 250 of the largest fintechs. Marquee customers include Chime, SoFi, Robinhood, Gusto, Public, Stash, DraftKings, State of California, and Florida's Homeowner Assistance Fund. Socure customers have become investors in the company including Citi Ventures, Wells Fargo Strategic Capital, Capital One Ventures, MVB Bank, and Synchrony. Additional investors include Accel, T. Rowe Price, Bain Capital Ventures, Tiger Global, Commerce Ventures, Scale Venture Partners, Sorenson, Flint Capital, Two Sigma Ventures, and others.