Socure™

EBOOK

How Legacy Identity Verification Vendors Expose Your Enterprise to Risk

Introduction

The challenges legacy identity verification solutions have been tasked to solve have grown increasingly complex

The strength of an identity verification solution is not determined solely by having more data than anyone else.

It is solved by combining the maximum amount of data to cover all ages, races, demographics, and genders with best-in-class entity resolution, clustering, and machine learning (ML) technology to resolve back and correlate to any given identity with the highest degree of accuracy and coverage. With this combination also comes the ability to identify and safely onboard more good customers, with the highest degree of precision possible. Simply put, organizations that are serious about delivering inclusive onboarding and achieving continuous compliance with increasingly stringent regulatory mandates have to operate with a solution that moves beyond the limited analytical capabilities of legacy identity verification solutions.

Many legacy identity verification solutions claiming "smart linking" technology were developed over two decades ago. While little has changed in their core functionality since then, the challenges they have been tasked to solve have grown increasingly complex, creating gaps in accuracy across name, address, phone, email, DOB, and SSN matching.

According to Socure research, this means that about 4% of all transactions are returning the wrong answer — at scale. For example, legacy vendors tend to claim exact DOB matching when in fact fuzzy matching is being performed because of sheer looseness in the algorithms. In another example, many legacy providers frequently classify an address as residential when it is actually something entirely different, like a commercial business or even a prison. Finally, legacy players often negatively impact Hispanic or Asian-descent individuals because of an inability to recognize and match on patterns of split names and concatenations.

Legacy solutions lack the accuracy of Socure

Socure's graph-defined identity verification platform analyzes the entirety of an individual's identity with ML to correlate the freshest and broadest set of data available to maximize accuracy and coverage, without introducing any friction into the customer experience.

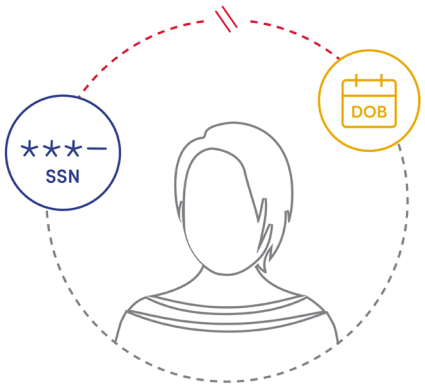
Through hundreds of customer data studies examined on a transaction-by-transaction basis, Socure can confirm that legacy KYC/CIP solutions are incorrectly returning matches ~4% of the time. These solutions are also unable to verify certain segments of the population across different ages, races, and socioeconomic classes more than 10% of the time. Needless to say, the adverse impact of these issues is massive. Even a seemingly small percentage of incorrect identifications over a large customer portfolio adds up to both an operational and regulatory nightmare, especially in an audit.

Digging deeper, in one examination of a sample customer file for a major fintech, Socure found that a shocking 40% of all applications approved by a legacy provider contained these issues:

- Customer approvals in conflict with the organization's stated KYC/CIP acceptable policy
- Verification and approvals on the wrong SSN, often times with edit distances >4
- Verification and approvals when the SSN was issued before the DOB
- Incorrect fuzzy matching on SSN where matches were claimed and the edit distance was ≥1
- Approval of deceased customers and associated SSNs
- Matching on secondary SSNs (in violation of CIP requirements)
- Address classification issues—P.O. box, commercial/business address/CMRA, business ZIP codes being returned as residential addresses which financial institutions require both for regulatory and mailing purposes
- Approval of government-sanctioned individuals

40% of all applications approved by one legacy provider contained issues

If you're currently using a legacy identity verification solution, you can expect to find many of the same issues in your own customer portfolio.



Example 1: Incorrect DOB and SSN match

The most basic and critical task that identity verification solutions must get right is complying with KYC/CIP regulations. If an incorrect identity is matched to a customer, the result is non-compliance. For organizations that require exact matching on DOB or SSN as part of their scorecard, our analysis has discovered that legacy solutions are matching the incorrect individual 3-4% of the time.

SSN before DOB

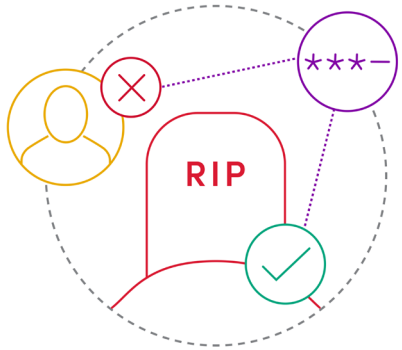
An issue Socure routinely sees is verification of is the verification of an SSN that was issued before the DOB, resulting in an approval. This can be a problem for customers with an SSN issued prior to 2011, as the birth date in part determines the makeup of the issued SSN. As an example, we identified a customer with a DOB of 07-28-1974, but the issue year of the SSN on file is 1972. Had the legacy provider accurately matched the DOB, it would have been easy to discover that the SSN was not a correct match—or at least it would have been able to flag the discrepancy.

Use of fuzzy matching and incorrect fuzzy matching

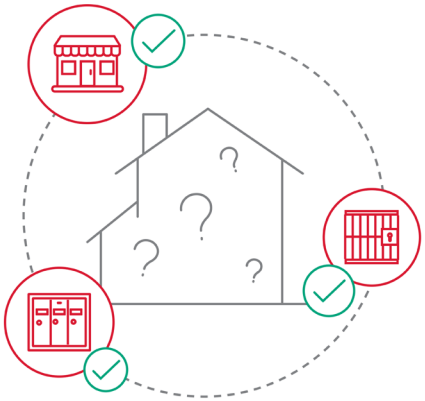
Some customer KYC/CIP policies mandate exact matching for the SSN and/or DOB. Despite this, our team regularly discovers that legacy solutions are either ignoring this requirement and using fuzzy matching when an exact match can't be found or they are incorrectly matching an SSN to a customer because of their algorithmic matching logic simply being outdated. In some cases, the approved SSN is off by one to two years from the DOB.

Example 2: Approval of deceased customers

Socure consistently discovers multiple instances of legacy solutions approving customers that are actually deceased, as well as the inverse, where customers who are living are declined for being deemed deceased. These instances typically involve more than one SSN tied to a customer, suggesting that the legacy solutions are matching individuals on secondary, non-primary SSNs.



Example 3: Incorrect address classification



In an actual customer data analysis for a top 10 banking institution, Socure found hundreds of instances of the bank approving customer applications where the customer address was a commercial mail-receiving agency, a violation of regulations requiring a residential address. And these errors were found in a small snapshot of their recent transaction data; the true risk of exposure is far more extensive.

But it gets even worse. Socure found actual examples in their customer data of the use of correctional institution addresses that were approved by their legacy identity verification solution as valid customer residential addresses. These "customers" provided addresses at correctional institutions in Pennsylvania and Indiana that should never have been approved.

Confirmed residential addresses via legacy solutions

Definitively resolving an address

Socure has the most accurate address matching in the U.S., with over 99.5% coverage—more than the USPS, Smarty, or even Google. Socure combines data from these and other sources for maximum coverage and then optimizes to a single normalization, ensuring you get the most comprehensive, accurate match. Regulated industries such as financial institutions that require a residential address for their customers can't afford to get this wrong.

Example 4: Approval of sanctioned individuals

With new sanctions imposed following Russia's invasion of Ukraine, regulators have greatly increased their focus on sanction and watchlist violations. This means that screening for sanctioned individuals is no longer simply a bureaucratic box to check, as these lists are continually updated and can present a serious, ongoing risk to your organization.

In a recent customer analysis for another top 10 bank, Socure found these three sanctioned individuals who were permitted to open accounts and transact in violation of applicable sanctions regulations:

1. A customer with criminal records from the Georgia Bureau of Investigation who matched on name and exact DOB
2. An approved applicant on the OFAC sanctioned list who matched on alias name and exact DOB
3. An approved applicant on Canada's OSFI Person List who matched on alias name and exact DOB

These were not all individuals trying to evade detection, as they used their actual name or a known alias as well as actual exact DOB, but were missed by the legacy identity provider. Of even greater concern is the reality that an auditor is going to ask, on a line-by-line basis, why sanctioned individuals were allowed to transact.

Socure is proven to be the most accurate identify verification provider

Socure's advantage comes through connections and correlations from that data, which are orchestrated and integrated into our proprietary matching capabilities

Aside from having the traditional sources used by most providers, Socure invests heavily in additional, redundant data sources from the most diverse, authoritative, and reliable sources. But while having diverse, in-depth data is essential, data volume can actually be a zero-sum game. More is better, but only to a degree. Data is only as useful as the insights that can be obtained from it. Socure's advantage comes through connections and correlations from that data, which are orchestrated and integrated into our proprietary matching capabilities.

For example, Socure uses 26 different name-matching algorithms, which make our industry-leading accuracy possible. And that's just one aspect of our patented identity clustering technique.

Additionally, Socure not only matches on multiple sources that have corroborated name, email, phone, address, DOB, SSN, and other PII elements such as IP and device, but we also have actual confirmation of a good or bad identity as reported by our customers (your peers) in our proprietary feedback data network of more than one billion known outcomes to compare against.

Data is only as useful as the insights that can be obtained from it.

Socure has built something unique in the identity verification market—our own, one-of-a-kind consortium of actual decision outcome data from more than 1,200 customers that provides us with specific, accurate decisioning data about good and bad identities and their outcomes. And it continuously learns more every day with each new transaction and each new customer who joins the Socure network, ultimately keeping our customers ahead of evolving risks to their business. No other provider in the market can truthfully make this claim.

We've built something unique in the identity verification market—our own, one-of-a-kind consortium of actual decision outcome data from more than 1,200 customers

Socure consistently delivers real auto-approval lifts of at least 7% when compared to any other provider in the industry. In a time when every customer is so valuable, and the frequency of audits are increasing substantially, accurately approving more customers and maintaining good customer accounts has never been more critical.

Socure's KYC solution offers access to the best-matched entity for every transaction—ensuring your confidence in exactly what data we matched against and delivering unsurpassed accuracy while reducing operational costs. In cases where manual review or reviewing the final disposition is required, both our dashboard review capabilities and API offer a side-by-side comparison of customer input data with the best-matched identity, with detailed reason codes and field validation scores providing the context needed to quickly focus on elements of risk to make a sound decision.

Last but not least, Socure can identify the risk that currently exists in your portfolio so you can take action and prevent new risks, while automatically approving more good customers. Our data science experts are ready to investigate a sample of your customer portfolio, with a row-by-row analysis to uncover incorrect classifications and identify where we can verify and approve additional customers so you can thrive in the current economic environment.

Ready to get started?

SPEAK WITH AN EXPERT

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 1,400 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.

4180571982 033023

Socure