



Digital Identity Verification in Financial Services

IMPLEMENTATION
STRATEGY GUIDE

Mitek

Digital identity verification in financial services

Today's consumers have come to expect seamless, frictionless experiences in their digital lives, and want no less when it comes to managing their finances.

To meet the rising expectations of digital-first customers, financial institutions (FIs) have moved quickly to deploy a wide array of services through online and mobile banking services.

As new digital services continue to evolve, one conundrum remains constant: how to deliver a fast, frictionless experience for customers while accurately stopping the relative few seeking to commit fraud.

Document-based digital identity verification paired with biometrics is an effective way to balance both objectives. In this guide, we'll share best practices gained from working with hundreds of financial institutions. We'll help you evaluate where it makes the most sense to implement digital identity verification (DIDV), and how to best evaluate the business impact of your particular implementation.

What's inside

This guide is designed to help financial institutions best implement digital identity verification in a variety of use cases – deposit accounts onboarding, loan originations, credit card applications, money transfers, and more.

The right time and place for digital identity verification

Where and how to introduce DIDV is guided by business objectives and a clear understanding of implementation considerations.

Over the past few years, consumers of financial services have become more comfortable with digital identity verification. For one reason, they've become more attuned to the need to protect their identity privacy. And at the same time, banks have found better ways to present IDs and biometrics verification – making it simpler and easier for customers.

Customers recognize that these extra steps are all a part of establishing trust and an ongoing relationship with their financial institution. In fact, 72% of US customers have indicated that they are willing to share more personal information if it means easier, secure access to accounts later.¹

Optimizing your DIDV implementation

Digital identity verification involves authenticating the identity document along with the biometrics presented (e.g. a selfie) to prove the user's unique, real-world identity. But now you've added extra steps that can be perceived as “friction” in the onboarding workflow or the point of sale (POS) transaction.

However, friction isn't always a bad thing. It can be an effective tool for protecting your business and creating trust in your brand.

The added level of friction in the customer experience is only one factor in your IDV implementation decisions. Once you are clear on business objectives – for example, is it more important to maximize new customer acquisition or reduce fraud? – you'll be able to balance other important implementation considerations:



Friction tolerance: How likely will users be willing to opt in – complete the verification step – rather than abandon the process?



Verification assurance: What is the tolerance for fraud risk with the transaction at hand? Document-based verification with biometrics produces a stronger trust signal compared to fraud detection signals relying on digitally accessible information.



Speed required : How quickly must the verification judgment take place? Will a response that takes more than a few seconds result in poor conversion or delay parallel risk scoring assessments within your platform?

¹2020 Global Identity and Fraud Report, Experian Information Solutions, Inc.



Implementation guidelines

DIDV as part of the customer journey
and back-end decisioning.



Front End: customer experience

When to introduce digital IDV in the user journey – early or late – can vary to support different use cases.

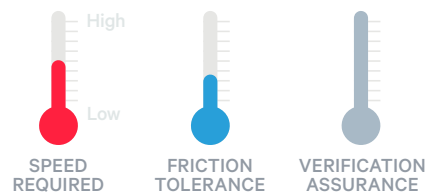
Business objective:

Considering factors:

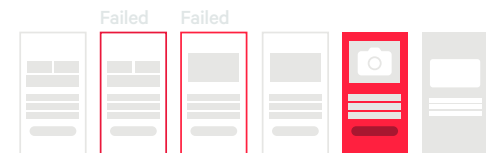
What the customer sees:

Maximize new user conversion

In use cases with low up-front monetary value or associated risk, most FIs want to provide potential customers with a convenient and streamlined first-time experience. Therefore, digital identity verification with biometrics is introduced as a backstop – when the person has failed initial passive, low-friction trust signals (static, behavioral, device data, etc.) Reserving DIDV only for those identity profiles with questionable reputation ensures that the vast majority of good applicants can complete the process in fewer steps.



■ DIDV
□ Other trust signals



In low-risk use cases, introduce DIDV as a backstop/failover (e.g., DDA onboarding)

Streamline regulated real-time transactions

For transactions that exceed specified risk thresholds, such as the size of the transaction or the type of transaction involved, FIs will employ digital identity verification as a required security check. With DIDV implemented at the “point of sale”, transacting customers avoid alternative filters for verifying their identities.



In transactional use cases, introduce DIDV at the point of sale (e.g., money movement)

Minimize fraud

In higher risk scenarios, FIs focus on minimizing fraud, and introduce digital identity verification as an initial entry point, in lieu of lower-friction trust signals which may be less effective in detecting bad actors. For these high value use cases, DIDV can be presented as “positive friction” – instilling trust from the start and streamlining future interactions with the FI.

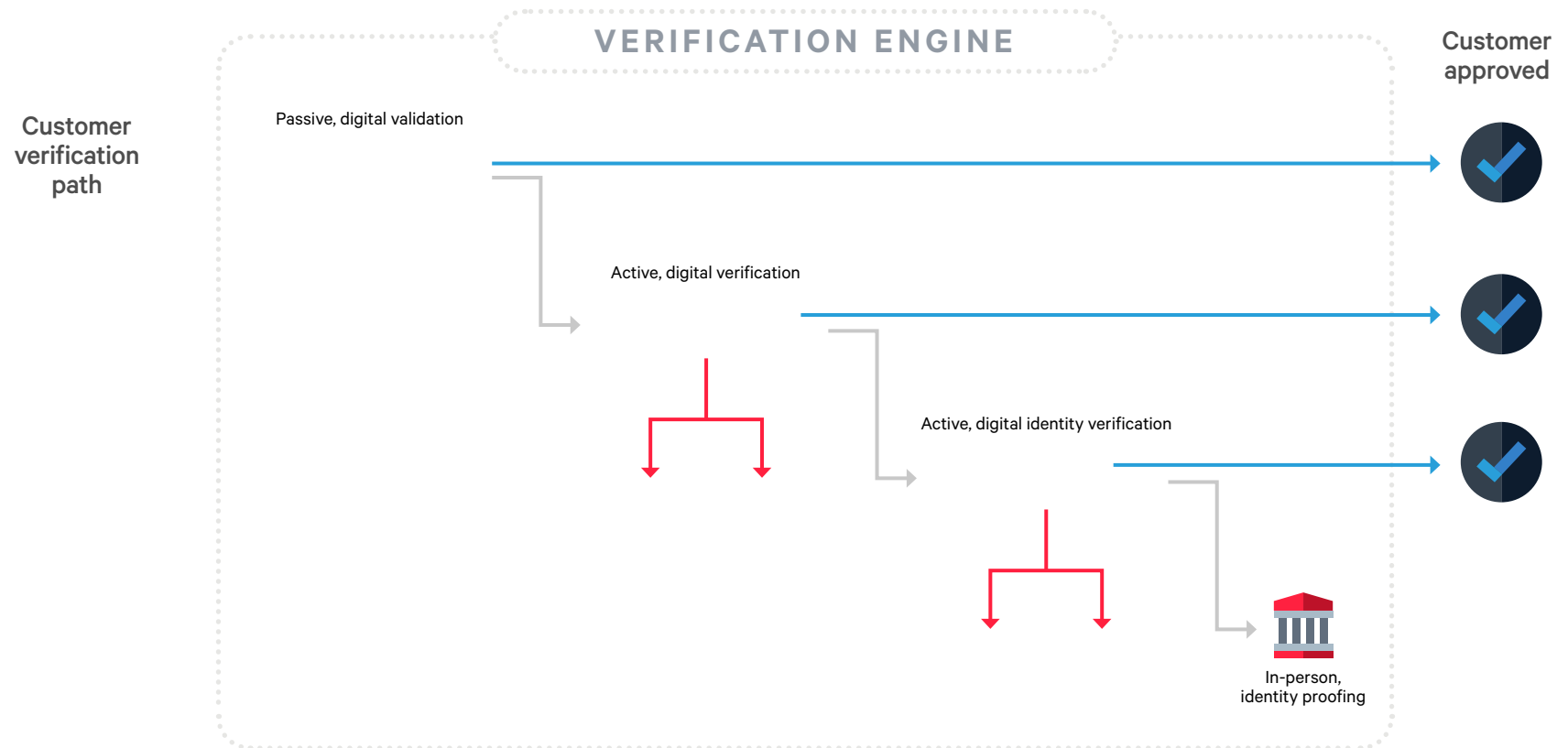


In higher risk use cases, introduce DIDV at the outset (e.g., credit line opening or loan originations)

Back End: **decisioning logic**

Understanding the capabilities of each of the following trust signal cohorts within your verification engine will help clarify the value of DIDV as 1. a backstop, 2. verification at the point of sale or 3. a way to mitigate risk at the outset.

Mouseover each symbol in the chart below for additional guidance.





Metrics that matter

Key metrics used by FIs when
evaluating DIDV solutions.



Which metrics **matter most?**

Many financial institutions, when evaluating digital identity verification solutions, tend to focus on the following metrics:

Approval rate: The percentage of customers whose ID and biometrics were deemed authentic, relative to the number of processable customer submissions (i.e., customers whose images were accepted).

Forgery detection rate: The percentage of forged documents detected accurately with respect to the entire number of accepted document submissions.

These are important metrics, but they don't fully represent the impact of digital identity verification to the customer journey and to your business.

Prioritize customers over fraudsters

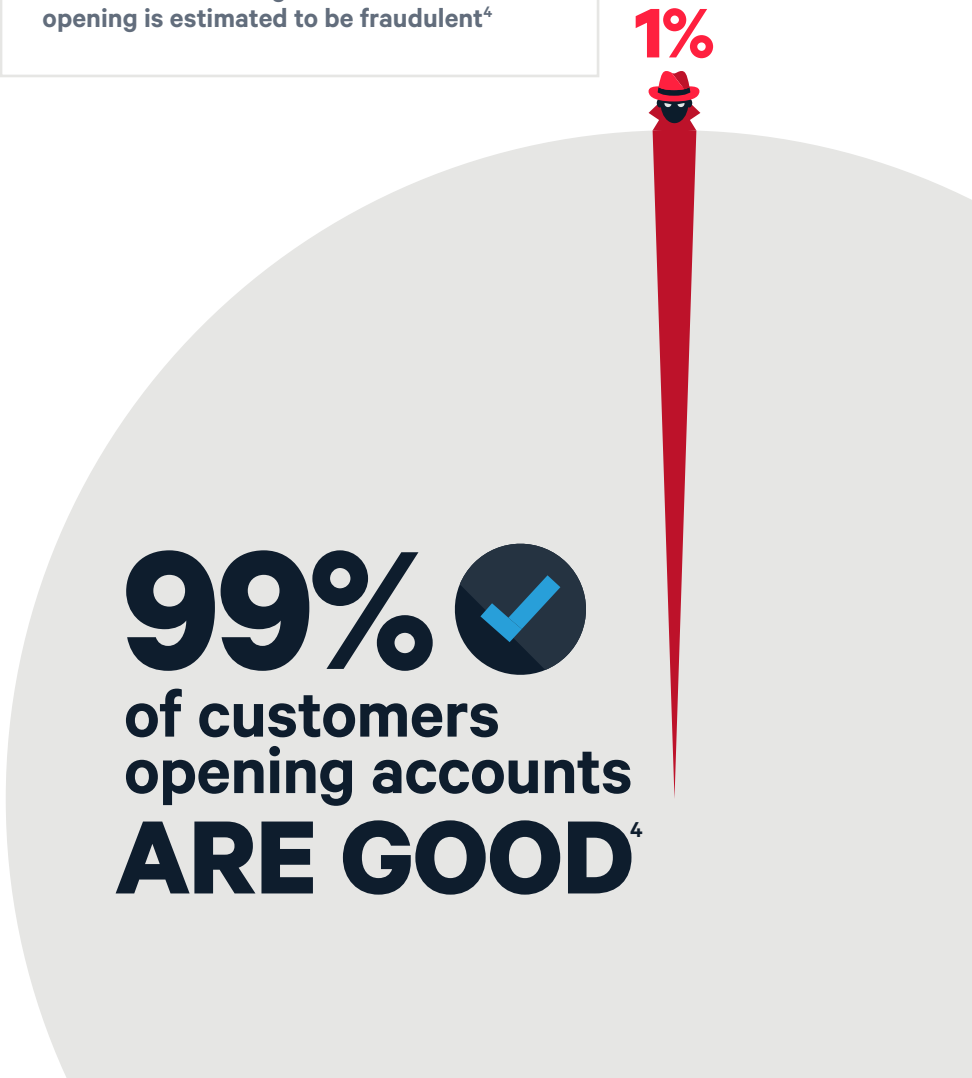
Prospective customers in the sign-up funnel are potentially the most valuable. Successful FIs have made this funnel into a flywheel – a great account opening and onboarding experience sets the tone for the experience throughout the customer's lifecycle.

According to Javelin, less than 1% of all new account openings are estimated to be fraudulent.⁴ This means that 99% of customers that open accounts are good. Wouldn't it make sense to measure the success of DIDV using this lens?

Evaluating identity verification solutions on the basis of how well they can detect fraud among the 1% of applicants who are actually fraudulent is like looking at the tip of the iceberg.

How well you are approving and onboarding the vast majority of good customers can have a far greater impact to your business.

- Lending fraud monetary losses amount for 2.9% of overall revenue²
- 0.9% – 2% identity theft incident rate in New Account Fraud (NAF) for Loan Products³
- 0.5% – 0.8% the range of new account opening is estimated to be fraudulent⁴



99% 
**of customers
opening accounts
ARE GOOD⁴**

1% 

The diagram features a large light gray circle representing the base of an iceberg. A thin red vertical line extends from the top of the circle, representing the tip of the iceberg. At the very top of this line is a small black silhouette of a person wearing a red hat and a mask. To the left of the circle, the text '99%' is written in large, bold, dark blue font, followed by a dark blue circle containing a white checkmark. Below this, the text 'of customers opening accounts ARE GOOD⁴' is written in bold, dark blue font. To the right of the circle, the text '1%' is written in large, bold, red font. The red vertical line is positioned to the right of the '99%' text and to the left of the '1%' text.

²Lexis Nexis study, <https://finance.yahoo.com/news/smaller-banks-credit-unions-digital-123000227.html>

³Digital Lending Fraud Report, Javelin, 2017 pg. 14&15

⁴Javelin Research: 2017 Identity Proofing Platform Scorecard, Oct 2017

Customer experience has a **higher impact** on your business

Accurately detecting fraud is crucial for banks, but successfully onboarding and servicing good customers is the far greater opportunity.

While product teams and risk managers may debate priorities, the success of DIDV must be considered holistically from an ROI standpoint.

Many banks continue to evaluate DIDV products with a focus on lab-handled performance metrics such as *forgery detection rate* or *insult rate* (i.e., wrongly rejecting good prospects). But lab tests alone won't help banks evaluate more important customer-centric success metrics that can only be tested with actual people.

Putting customer experience at the forefront of your digital identity verification evaluation criteria is likely to have a far greater impact on your business than simply detecting fraud. According to Gartner, by 2022 digital businesses with great customer experience during identity corroboration will earn 20% more revenue than comparable businesses with poor customer experience.



+20% MORE REVENUE

can be captured by companies with a great identity corroboration experience.⁵

A more comprehensive evaluation considers key metrics associated with both customer behavior and back-end decisioning:

Opt-in rate: The percentage of customers who decide to continue with the process and capture ID and selfie. Also known as click-through rate.

Completion rate: The percentage of customers who completed the process, successfully capturing ID and selfie images for the system to process, regardless of whether they were authentic or fraudulent. The opposite from completion rate is known as abandonment rate.

Approval rate: The percentage of customers whose ID and biometrics were deemed authentic, relative to the number of processable customer submissions. Those excluded in this step are either forgeries or faced a processing issue.

Conversion: The percentage of customers whose identities are deemed authentic and have proceeded to finalize the onboarding process or transaction.

⁵"Gartner, Inc. Don't Treat Your Customer Like a Criminal", Published: 28 April 2017, ID: G00324125, Analyst(s): Tricia Phillips



Evaluation best practices

How to plan and prepare for a
successful DIDV evaluation.



How to evaluate DIDV **holistically**

We've worked with hundreds of FIs to help them evaluate and integrate digital identity verification into customer onboarding or transactional workflows. We encourage a holistic approach that helps our clients balance customer experience with fraud assurance.

Define goals and target metrics

We start by understanding your business goals, which can help determine what is most important to test and measure. If your goal is to minimize fraud, processing speed may be less important. On the other hand, if your main objective is to streamline real-time transactions, verification speed may be one of the most critical success factors.

Pilot or POC?

A proof of concept (POC) is generally smaller in scope than a pilot and can be conducted with fewer resources and completed faster. It usually involves testing on lab-generated data and images. A POC can verify how well a digital identity solution detects fraudulent IDs; however, a POC does not help you test how well a digital identity verification solution is able to approve and onboard desirable customers.

A pilot is a controlled rollout of digital identity verification for a specific use case. Often deployed in a production environment, it uses real-life user data and helps you evaluate how well the solution will work in the actual world. A pilot can help FIs test a

greater variety of customer success metrics, including how many customers start an onboarding process and make it through the entire process, how many customers abandon the process, and how many get accepted and approved. While pilots may take longer to complete or require more resources to conduct, they portray a more complete view of the business outcomes.

	POC	Pilot
What test data is used?	Limited, static and lab-generated	Real-life user data
Development resources required	Fewer	More
How much of the DIDV solution is tested?	Speed and fraud detection only	End-to-end user journey
What success metrics can be measured?	Fraud detection accuracy	Abandonment, image acceptance, approvals, conversion rates and others

Pilots vs. POCs

A POC can verify how well a digital identity solution detects fraudulent IDs. For customers that want to obtain a more holistic view of digital identity verification and success metrics, a pilot is a more effective choice. It uses real-world data and creates a representative test of the entire conversion journey – from completion to conversion.

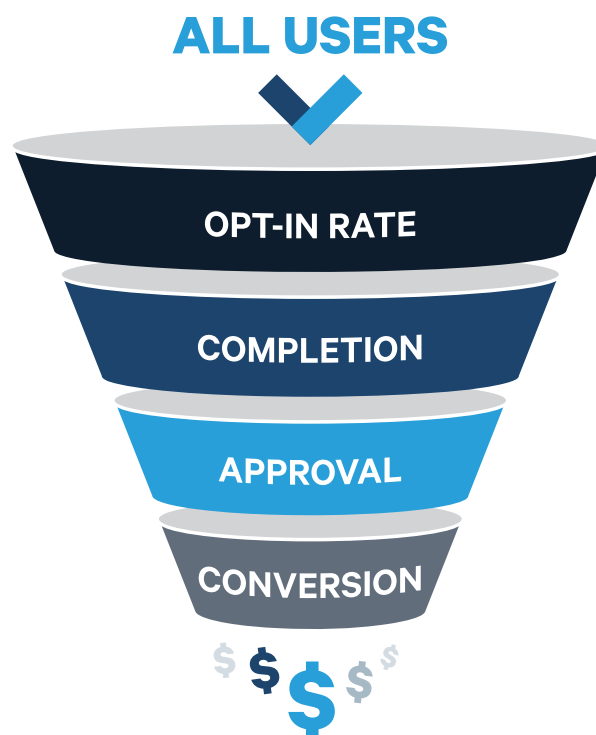
PROOF OF CONCEPT

Non-applicable, since this testing doesn't involve end users

Often performed with small sets of lab-generated images, which don't replicate real-life user submissions

Lab-generated images tend to be forged in ways that may not reflect what fraudsters in fact do in real life

Non-applicable, since POCs do not offer an end-to-end view of the user conversion journey



PILOT TESTS

Evaluate and optimize before general availability

Contained, yet uncontrolled real-life photo submissions

Forgery detection, FNR, others can still be measured through human expert corroboration

Pilots let you see how many users start and how many make it through

How to plan and prepare for a **successful pilot** evaluation

Successful pilots require detailed project plans, with the vendor and customer sharing their experiences. This ensures the best outcomes when the digital identity verification solution is launched.

Companies who conduct a pilot with Mitek can expect the following sequence of events:

Kickoff: Confirm use cases and products. Detail project timelines. Define and agree on success criteria. Schedule engagement cadence throughout implementation and post launch.

Implementation and training: Implementation guidance for technical and business staff. Cross-functionally align on project plan and timing based on resource availability.

Prelaunch: Clearance of final details based on specified customer requirements. Define and present contingency launch plans.

Day of launch: War room established with live – or preferred cadence of – communication..

Post launch: Weekly status checks to review determined success criteria.

Review: Evaluate success criteria versus pilot performance. Assess risks and viability for technology integration.

STARTUP



Kickoff



Implementation
Training

IMPLEMENTATION



Prelaunch



Launch
Day



Post
Launch

OPTIMIZATION



Pilot
Review



About Mitek

Mobile Verify®, Mitek's premier digital identity verification product, is trusted by digital leaders for its proven, customer-centric user experience. This solution is used by leading brands across the globe to create trust in the digital channel for safe, convenient customer onboarding, fast money movement, and user authentication.

Digital leaders trust Mitek's Mobile Verify because it keeps them in compliance with ever evolving Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations.

Using patented science, Mobile Verify validates that the government issued ID presented in a digital transaction is authentic and unaltered. As a second layer for identity proofing, Mobile Verify uses sophisticated face comparison algorithms to automatically compare the portrait extracted from the ID document with a selfie; proving that the person submitting the ID document is its rightful owner. This enables your enterprise to onboard more good customers while meeting compliance.

Optimize your customer journey with DIDV.

See how Mitek can help.

go.miteksystems.com/demo