ID Verification

Contents

[Pros and Cons of ID Verification 1](#_Toc178016195)

[Pros of ID Verification: 1](#_Toc178016196)

[Cons of ID Verification: 2](#_Toc178016197)

[Implementing ID Verification 3](#_Toc178016198)

[Costs of ID Verification 7](#_Toc178016199)

[Smile ID 7](#_Toc178016200)

[iDenfy 9](#_Toc178016201)

[Jumio 11](#_Toc178016202)

# Pros and Cons of ID Verification

## Pros of ID Verification:

1. **Enhanced Security and Privacy:**
   * Ensures that only authorized users access sensitive personal and medical information, protecting users' privacy.
   * Helps comply with data protection regulations (e.g., HIPAA in the U.S., GDPR in the EU), minimizing the risk of legal penalties.
2. **Fraud Prevention:**
   * Reduces the likelihood of fraudulent use of medical services and prescription forgery by verifying the identity of both patients and healthcare providers.
   * Adds an additional layer of protection to ensure that prescriptions are not misused or altered.
3. **Trust and Credibility:**
   * Establishes trust among users, who are more likely to engage with a platform that ensures their medical data is secure.
   * Increases the credibility of the app, especially when dealing with sensitive information like prescriptions.
4. **Regulatory Compliance:**
   * Demonstrates adherence to healthcare industry standards and legal requirements for handling medical data, which is critical in gaining approval from healthcare institutions and insurers.
5. **Accurate Record Keeping:**
   * Ensures that prescriptions and medical records are correctly attributed to the right patient, reducing errors in patient care.

## Cons of ID Verification:

1. **User Experience Friction:**
   * Adds extra steps to the onboarding process, which could deter some users from signing up or using the app.
   * Some users may find it inconvenient or confusing, especially if the process is overly complex or time-consuming.
2. **Cost and Complexity:**
   * Implementing ID verification requires integrating with third-party services or building an in-house system, both of which add development costs.
   * Ongoing maintenance and updates to the verification system will also increase operational costs.
3. **Potential Exclusion of Some Users:**
   * Users without access to necessary identification documents or those unfamiliar with digital verification methods might be excluded or face barriers to accessing the app.
4. **Security and Privacy Risks in Verification Process:**
   * Although ID verification enhances security, improperly storing or transmitting verification data (like scans of IDs) can create new security vulnerabilities.
   * If third-party ID verification services are used, there’s a dependency on their security practices, which adds risk.
5. **Legal and Ethical Considerations:**
   * Handling sensitive identification data may involve complex legal obligations, and any breach could result in serious legal ramifications.
   * Ethical concerns arise around how user data is used and whether users are aware of and consenting to how their data is handled.

By balancing these pros and cons, you can determine the most suitable approach for incorporating ID verification into your healthcare app. It's important to ensure the verification process is secure yet user-friendly, while remaining compliant with relevant healthcare and privacy laws

# Implementing ID Verification

Implementing ID verification in a mobile app, especially in a healthcare context, requires a well-thought-out approach that balances security, compliance, and user experience. Here's the best way to do it:

**1. Define Requirements and Objectives**

* **Security:** Ensure the system provides robust identity verification without exposing sensitive data.
* **Compliance:** Comply with healthcare regulations (e.g., HIPAA, GDPR) regarding data handling and storage.
* **User Experience:** Make the process seamless for users to avoid drop-offs during registration or use.

**2. Choose the Type of ID Verification**

* **Document Verification:** Users upload a government-issued ID (e.g., passport, driver’s license) and the app verifies the document’s authenticity.
* **Biometric Verification:** Use facial recognition or fingerprint scanning to match the user’s ID photo.
* **Two-Factor Authentication (2FA):** Implement 2FA to verify user identity with an additional code sent via SMS, email, or app-based authentication.
* **Knowledge-Based Verification (KBA):** Ask users specific personal questions that only they would know.
* **Real-Time Identity Verification:** Cross-reference user information with government databases or credit bureaus for instant validation.

**3. Use a Trusted Third-Party Provider**

Implementing ID verification in-house can be complex and risky. It’s more efficient to use a third-party provider that specializes in identity verification, such as:

* **Jumio:** operates in over 200 countries and territories, including South Africa, offering ID verification, biometric checks, and anti-money laundering (AML) compliance solutions. It supports a wide range of government-issued IDs and ensures compliance with regulations such as GDPR and AML​ ([Jumio](https://www.jumio.com/industries/" \t "_blank)) ​([Jumio Verification](https://go.jumio.com/id-kyc-comps" \t "_blank)).
* **Onfido:** is also available in South Africa and provides identity verification using document scanning and biometric checks. It uses AI-powered technology to reduce fraud and ensures compliance with local and global regulations​ ([Onfido](https://onfido.com/jumio/" \t "_blank)).
* **Smile ID:** Smile ID offers identity verification solutions specifically tailored for Africa, including South Africa. Their key features include:
  + Document verification for South African IDs, passports, and driver's licenses
  + Biometric facial recognition with 99.8% accuracy for African faces
  + Government database checks
  + Mobile SDK for easy integration into apps
  + AML and fraud screening capabilities
* **Uqudo:** uqudo provides digital identity verification services for South Africa with the following offerings:
  + Verification of South African national ID cards, passports, and driving licenses
  + AI-powered document scanning and data extraction
  + Facial recognition and liveness detection
  + Integration via mobile SDK
  + AML screening
* **Secure Citizen:** As a South African company, Secure Citizen offers identity verification tailored for the local market:
  + Verification against South African government databases
  + Mobile API for app integration
  + Partnership with South African Fraud Prevention Service for added security
  + Focus on compliance with local regulations like POPIA
* **iDenfy:** While not South Africa-specific, iDenfy provides global ID verification that supports South African documents:
  + Verification of 3500+ document types including South African IDs
  + Mobile SDK for iOS and Android apps
  + Liveness detection and facial biometrics
  + AML screening capabilities

When choosing a provider, key factors to consider are:

* + Support for South African identity documents
  + Integration options for mobile apps (SDKs, APIs)
  + Compliance with local regulations
  + Accuracy rates for African users
  + Additional features like AML screening

These platforms typically provide document scanning, biometric verification, and database checks to ensure security and compliance. For a healthcare app, the choice between these services would depend on specific requirements but Smile ID or Secure Citizen might have a slight edge due to their focus on African markets and compliance with local regulations. Smile ID's high accuracy rate for African faces and Secure Citizen's partnership with the South African Fraud Prevention Service could be particularly valuable in a healthcare context where accurate identification is crucial.

**4. Implement a Seamless User Flow**

* **Onboarding Process:** Introduce ID verification during onboarding or sign-up. Inform users clearly why ID verification is required and how it benefits them (e.g., securing medical records).
* **Step-by-Step Guide:** Guide users through each step of the verification process, from scanning their ID to completing biometric verification.
* **Provide Feedback:** Offer real-time feedback to users, such as notifying them if their ID is successfully scanned or if they need to retake a photo.

**5. Security and Privacy Measures**

* **Data Encryption:** Encrypt all personal and ID data both in transit and at rest using secure encryption protocols (e.g., AES-256).
* **Compliance with Regulations:** Ensure the verification process adheres to healthcare regulations (HIPAA, GDPR). Avoid storing sensitive data longer than necessary.
* **Privacy Policies:** Be transparent with users about how their data will be used, stored, and protected. Obtain explicit consent before collecting any ID data.
* **Tokenization:** Use tokenization to store sensitive information. Instead of keeping actual data, store tokens that can only be decrypted by your verification service.

**6. Multi-Layered Verification**

* **Combine Document & Biometric Verification:** For extra security, require both document and biometric verification (e.g., scanning a government ID and performing a live facial scan).
* **Risk-Based Authentication:** Use adaptive authentication that increases security based on the level of risk (e.g., if a user logs in from a new device or unusual location, request additional verification).

**7. Test for User Experience**

* **Minimize Friction:** Test the process to ensure that it is as simple and quick as possible. Long or complex verification processes can deter users.
* **Offer Support:** Provide clear instructions and offer customer support if users run into trouble during the verification process.

**8. Monitor and Update**

* **Fraud Detection:** Regularly monitor the ID verification process for suspicious behavior and improve detection algorithms to prevent fraud.
* **Stay Updated:** As ID verification technology evolves and new regulatory requirements emerge, ensure your system is updated to meet the latest standards.

**Implementation Process Flow Example:**

1. **User Onboarding:** A user creates an account and is prompted to verify their identity.
2. **Document Upload:** The user scans a government-issued ID (driver’s license, passport).
3. **Biometric Scan:** The user is asked to take a live selfie or scan their fingerprint.
4. **Data Validation:** The system cross-references the document with the biometric data and possibly external databases.
5. **Verification Result:** The system provides real-time feedback, approving the user or asking for additional verification.
6. **Access Granted:** Once verified, the user gains full access to the app’s features.

By following these steps, you can implement a secure and user-friendly ID verification system that aligns with the healthcare industry’s strict security and privacy requirements.

# Costs of ID Verification

## Smile ID

<https://usesmileid.com/solutions/document-verification>

Smile ID offers flexible pricing options:

1. Pay-As-You-Go Plan:
   * Recommended for startups looking for a flexible solution
   * Full access to all Smile ID products
   * User portal with built-in analytics
   * Unlimited free test jobs in sandbox environment
2. Enterprise Plan:
   * Recommended for businesses verifying over 5,000 users per month
   * Includes everything in the Pay-As-You-Go Plan
   * Unlocks volume-based discounts
   * Dedicated account manager with Slack support channel
   * Technical integration support
   * Option to pay in local currency (for local companies)

Smile ID also offers a "**Smile for Success**" program for eligible startups, which includes:

* $6,000 in usage credits for Smile ID services.
* Up to 30,000 free KYC (Know Your Customer) checks.
* Access to all Smile ID solutions.
* One-on-one support.

The program is designed to help startups easily access identity verification services for their platforms. To be eligible for the program, startups must meet certain criteria, such as:

* Having launched their product within the last two years and onboarding at least 2,000 users per month

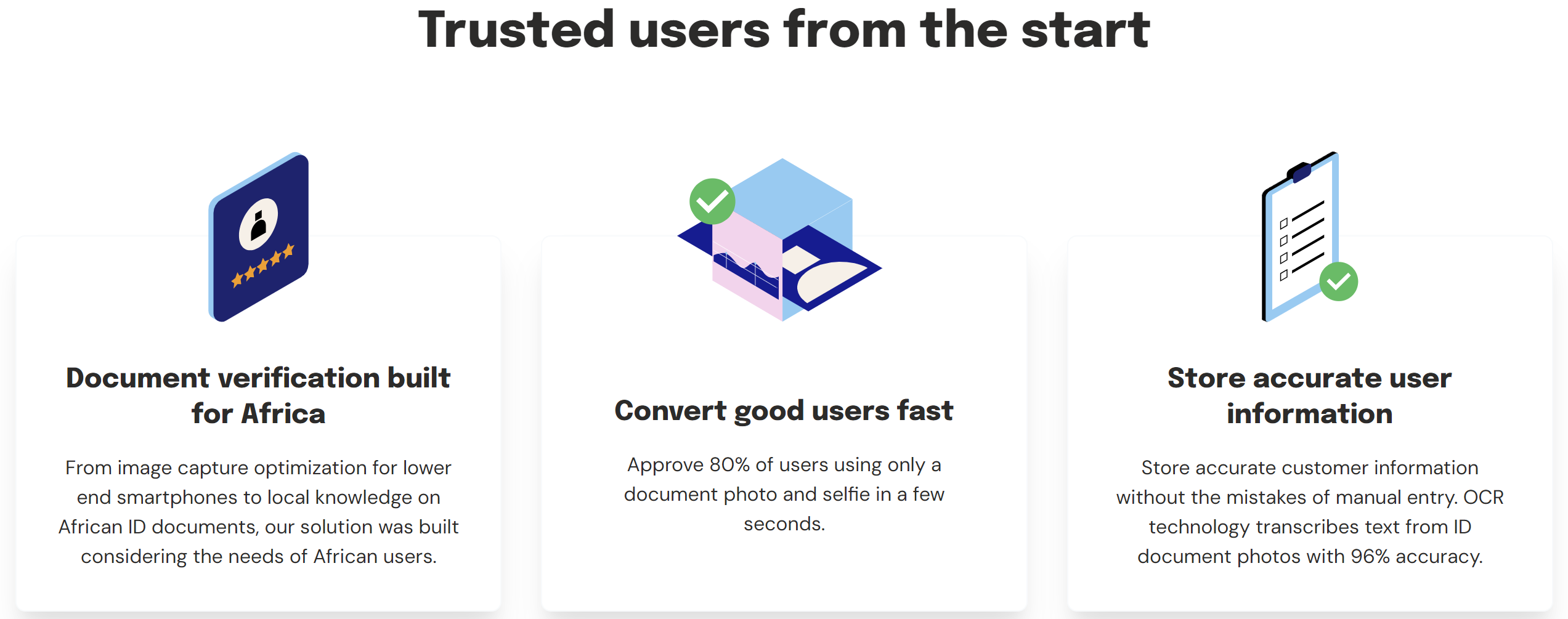
OR

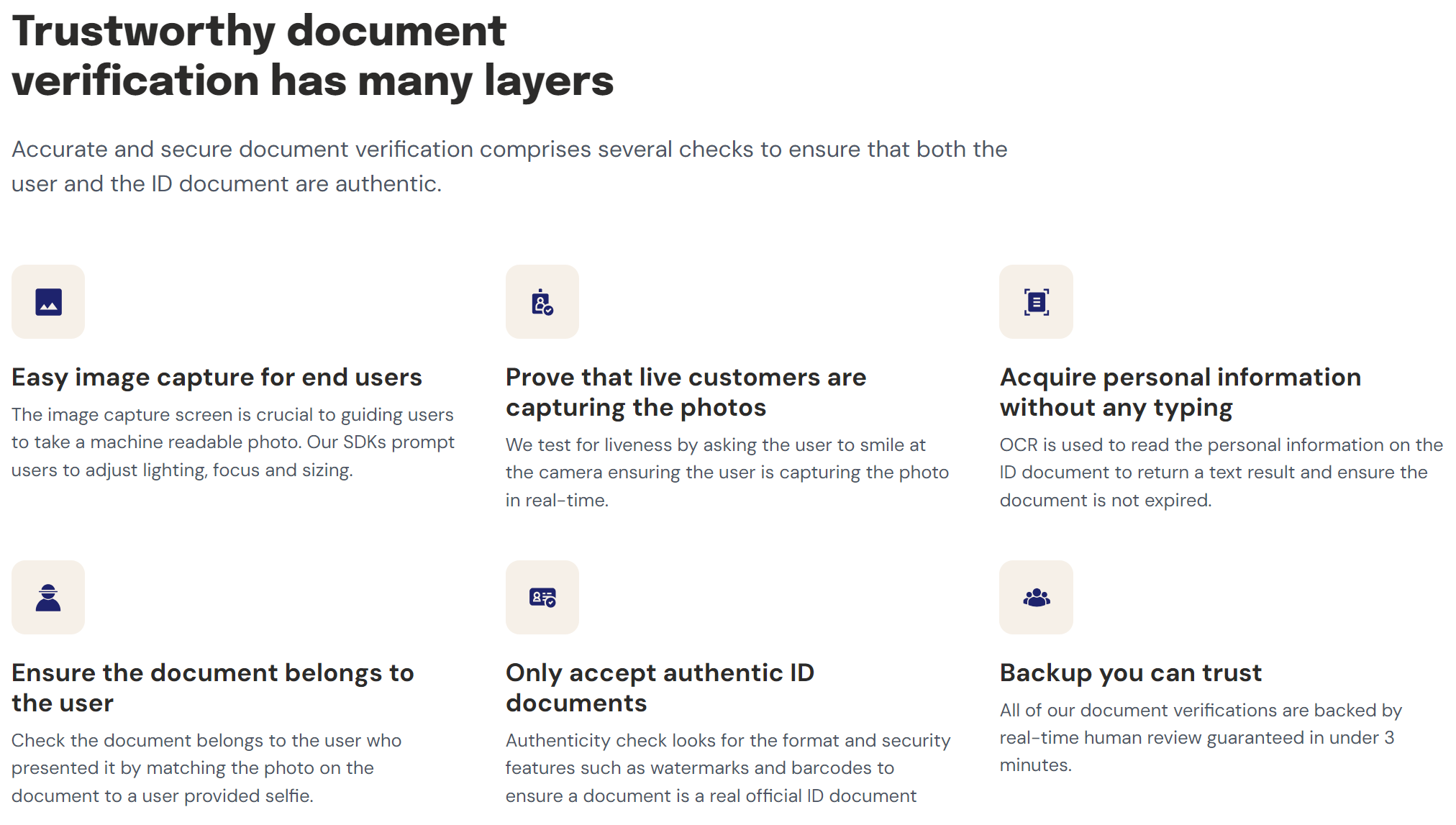
* having raised between $1 million and $5 million in funding

OR

* being recommended by one of Smile ID's partners

Additionally, applicants must not be current Smile ID customers and must be ready to integrate Smile ID within six weeks of being accepted into the program.This program aims to provide startups with affordable access to KYC compliance and onboarding services, which can often be costly for new businesses.





## iDenfy

<https://www.idenfy.com/>

iDenfy uses a cost-saving model where you only pay for successful verifications:

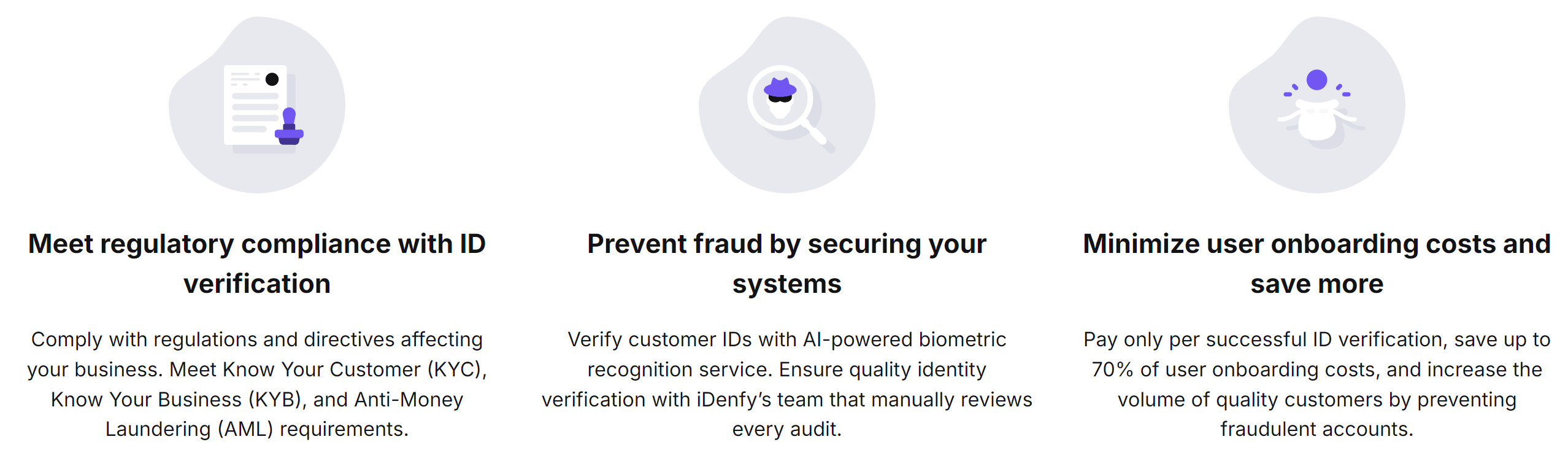
* Customers can save up to 75% on verification costs compared to paying for all verification attempts
* iDenfy covers the costs of denied identity verifications due to issues like blurry images, expired documents, or attempts from blacklisted countries
* They claim to help businesses save up to 70% on user onboarding costs

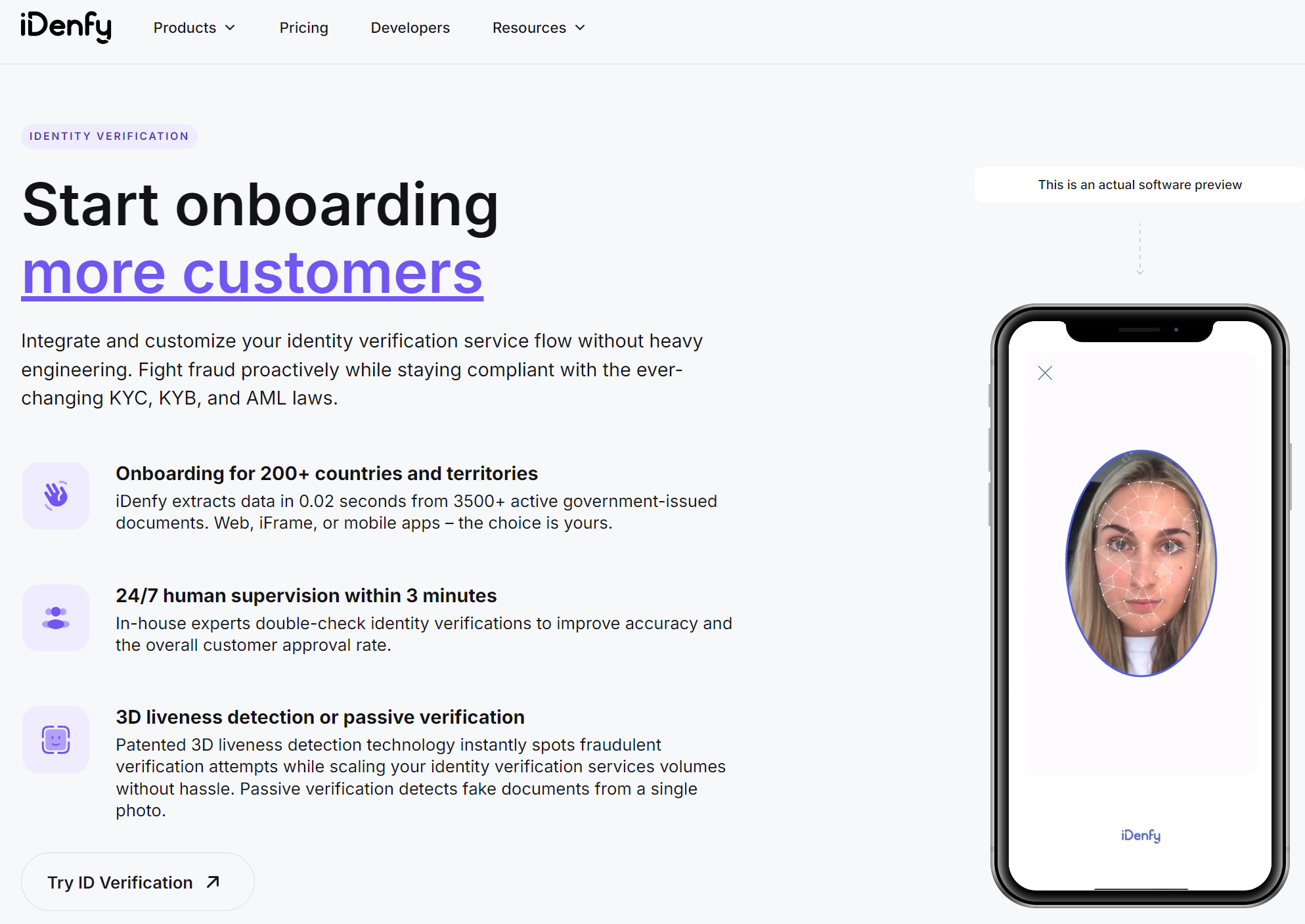
Key Considerations

1. Volume-based pricing: Both services likely offer better rates for higher verification volumes.
2. Success-based pricing: **iDenfy's** model of only charging for successful verifications can be cost-effective, especially if you expect a high rate of failed verification attempts.
3. Additional features: Consider the costs of extra services like AML screening, business verification, and ongoing monitoring, which may be priced separately.
4. Integration costs: Factor in any potential costs associated with integrating these services into your mobile app.
5. Customization: Determine if there are additional costs for customizing the verification flow or user interface to match your app's branding.

A screenshot of a phone

Description automatically generated





To get exact pricing, you'll need to contact these companies directly, as they don't publicly list their specific rates. It's recommended to request quotes from multiple providers and compare them based on your expected verification volume and specific requirements for your healthcare app.

## Jumio

