Uniquely you: Why biometric verification is key to proving digital identity

onfido

Tap, tap.
Who’s there?

Businesses in every industry are moving to digital models. From applying for a loan to shopping for groceries to getting a ride across town, companies are using digital infrastructure to connect people with what they want and need right now. But even as this opens up exciting possibilities, it also comes with a not-so-hidden risk: Identity fraud.

Fraudsters are taking advantage of the shift to digital to exploit vulnerabilities in identity verification (IDV) methods. It’s a problem that continues to grow, as criminals try to stay a step ahead and reap the benefits.

16.7 million

victims of identity fraud in the U.S. alone[2]

$2.1 billion

estimated global cost of data breaches by 2019

The high cost of knowing for sure

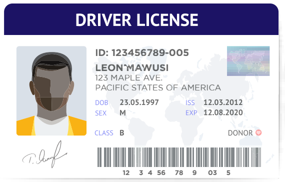
Traditional methods of verifying identity are costly, time-consuming, and fallible — which creates a big challenge for companies that want to acquire new customers. Even digital methods are imperfect, as not all verification processes are built for the fast-moving digital world. What happens when it’s glitchy and slow? Customers drop out or give up, which leads to onboarding fewer users, lost revenues, and wasted marketing spend.

Three elements of identity verification

Sorting genuine humans from fakes is a challenge that requires an advanced set of tools. Today, there are three key areas of focus in identity verification:

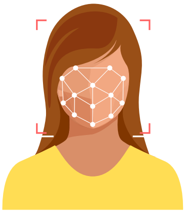
1. Personal data

Personal details form the baseline for identity verification, and are still used by many password systems. This data includes things like date of birth, social security numbers, past addresses, known associations, and more.



2. Identity documents

Identity documents, which we call IDs, are issued by a credible institution and help to verify identify. Validating these documents involves capturing their type, version, and information, and verifying them with the issuing authority, such as a government agency or financial institution.



3. Biometrics

Unique physical characteristics and human movements are important markers of identity. From facial analysis to voice recognition, biometric verification techniques to supplement and improve identify confidence.

These three layers can be used together or independently, depending on the use case and based on your risk appetite.

Why use biometrics as a part of identity verification?

How biometrics help solve a complex part of identity verification

When you ask for a user's name, date of birth, and address – and compare that data to what is held by a credit bureau, you're only able to protect against fake data. This information doesn't protect you against fake identities. In a world where people can go onto the dark web and buy data from anonymous oruntraceable sources, you need a way to defend against identities that easily pass a credit bureau check.

If you ask for an ID, the risk of impersonation risk drops. However, it's nearly impossible to detect IDs that haven't yet been reported as stolen or added to a law enforcement database. For example, a kid who wants to gamble online can easily use a parent's ID to set up an account. Similarly, someone underaged can "borrow" an ID to rent a car. Unless the ID has been reported as stolen, the fraud won't be detectable.

What can you do? Enter biometric verification.

Facial biometrics can be used to prove the ownership of a government-issued identity document. It compares the facial characteristics of the user presenting the ID document with the ones on the document itself.

Fake details– e.g., SSN, name, date of birth, address

✓ **DETECTABLE**
by an identity database

Stolen details, fake document

✗ **UNDETECTABLE**
by an identity database

✓ **DETECTABLE**
by document verification

Stolen details, stolen document

✗ **UNDETECTABLE**
by an identity database

✗ **UNDETECTABLE**
by document verification

✓ **DETECTABLE**
by biometric verification

But what happens if a selfie can be spoofed?

When it comes to biometric fraud, criminals are endlessly creative. From amateur attempts to highly sophisticated technical ones, there are many ways to impersonate a real identity or invent a false one.

Leveling up: From simple to advanced biometric fraud[1]

Level 1	**Common impersonation fraud** Fraudsters leverage printed photos or readily-available photos or screenshots from the web, including social media profile pics.	TIME short EXPERTISE anyone EQUIPMENT readily available
Level 2	**Sophisticated impersonation fraud** Fraudsters use digital tools to alter their own faces and other faces, and re-publish them as photos or videos.	TIME >3 days EXPERTISE moderate skill and practice needed EQUIPMENT available but requires planning
Level 3	**Highly-sophisticated impersonation fraud** Fraudsters use advanced 3D printing technologies to create a 2D mask of a face, cutting out eyeholes so that they can respond to commands from an eyeball tracking solution.	TIME >10 days EXPERTISE extensive skill and practice needed EQUIPMENT specialized and not readily available
Level 4	**Deep fakes (video impersonation)** The fraudster controls a live video of someone else's face, along with a realistic live voice that is mapped to facial gestures.	TIME >10 days EXPERTISE extensive skill and practice needed EQUIPMENT specialized and not readily available

How to evaluate solutions for biometric verification

When you're looking for a biometric verification solution, there are three key factors to consider.

1. Cross-channel & device support

Your customers expect a seamless experience across channels and devices, from native mobile devices to web browsers to cross-devices. Fraudsters know this, and are looking for gaps where spoofing techniques won't be caught on a particular device or channel. That's why it's important to have a solution that provides consistent identify verification across devices and channels.

2. Options that adapt to your risk appetite

Not all customers or situations are the same. You might want to put different types of customers through different levels of verification. That's why it's important to find a solution that has multiple options for biometrics and verification – so that you can adjust to balance risk appetite and end-user friction.

3. A model that drives a balance of fraud prevention, user experience, and scalability

In an industry where fraud evolves on a daily basis, how can you keep up with new fraud techniques? How can you also create a seamless user experience during customer onboarding that minimizes rejection and drop-off? Finally, how do you verify customers cost-effectively, without driving up customer acquisition cost as you expand into new regions or experience spikes in volume? The balance is tough, and you need a technology partner that can help you achieve all three.

Real or fake? Onfido knows.

Onfido provides a flexible, yet powerful solution for identity verification that matches your risk appetite and helps you minimize end-user friction. We provide two options for biometric facial analysis that you can choose based on the level of assurance you need.

Selfie Verification

This is the simplest option, guaranteed to provide the smoothest experience with the least customer friction and decent fraud coverage. In addition to a document photo, the user is also asked to take a selfie. That's all that is required of them. Available via our native mobile SDKs, our web JS SDK, or via direct integration with our well-documented API, this check compares the ID to the selfie and is for low-risk users or transactions.

Liveness Verification

This option eliminates the risk of spoofing, and keeps sophisticated fraudsters out. It's ideal for high-risk users, high-risk transactions, or for geographies with strict regulatory requirements. This method is the closest thing to meeting face-to-face without the burden of having a brick and mortar shop. Instead of taking a selfie, the user films themselves reading out numbers and performing randomized movements. It delivers high anti-spoofing assurance, while balancing user experience.

Deep dive: Selfie verification

Here’s how Onfido’s method for selfie verification works:

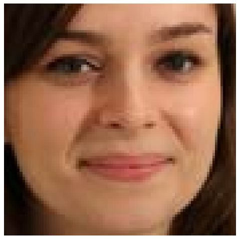
The photo on the identity document is extracted and compared with the face on the selfie, yielding a similarity score. Our proprietary algorithm has been trained to compare the face in the identity document with the selfie, and return a similarity score from 0 to 1.

The selfie is analyzed for abnormal texture, such as photos of photos, or photos of screens. Our proprietary, texture-based anti-spoofing technology detects photos of photos, even in the most challenging lighting conditions.

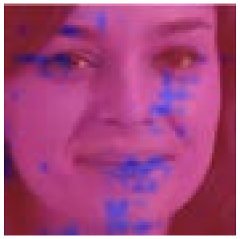
If any of our algorithms indicate a possibility that the selfie is fraudulent, we escalate it to our expert reviewers, including super recognizers.

The result: Highly accurate face matching and spoofing detection that gives you total assurance about user identity.

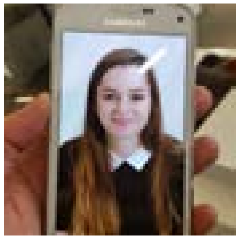
Genuine selfie



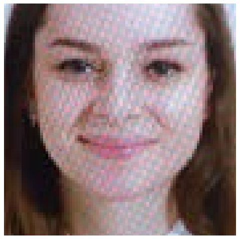
Face detection



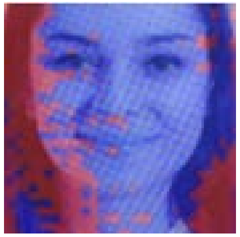
Spoof heatmap



Picture of a screen



Face detection



Spoof heatmap

Onfido has found that off-the-shelf solutions failed to detect faces on documents about 10% of the time, due to security features such as holograms that partially obstruct the face.

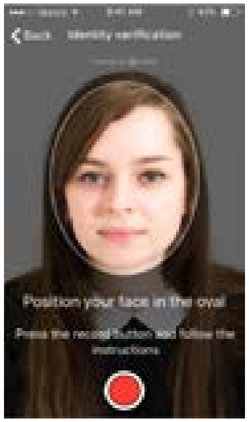
Deep dive: Liveness verification

Onfido's approach to liveness verification, also known in the industry as "proof of life," is based on a challenge-response mechanism.

Here's how it works:

- Applicants are required to film themselves while performing a set of simple but randomly-generated instructions, also known as challenges.
- These challenges include reading a random 3-digit sequence aloud, and performing a simple head movement. These ensure that the person is really alive and prevent even the most sophisticated spoofing attempts.

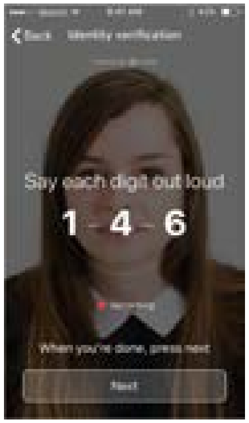
To aid the randomness, each retry generates a new challenge. The order of the challenges is also randomized. Sometimes it will ask for digits first; other times, a head movement first.



Back Identity verification

Position your face in the oval

Press the record button and follow the instructions



Back Identity verification

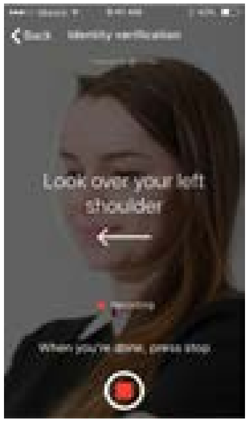
Say each digit out loud

1 - 4 - 6

Recording

When you're done, press next

Next



Back Identity verification

Look over your left shoulder

←

Recording

When you're done, press stop

How did we design these challenges?

Digit Challenge

By randomly using three digits, we've made it hard to spoof because there are so many possibilities. In addition, foreign speakers are more likely to know how to pronounce numbers, and accents are less likely to be a problem.

Head Movement Challenge

The randomness aspect of this challenge makes it especially effective. We also designed it to prove they are a live human, and stop anyone wearing a 2D mask by capturing a 3D video of their face. That's because fraudsters are highly unlikely to have a video of the person they are impersonating talking, then turning their head to one direction. It also allows for a backup method when sound quality is poor.

Onfido’s multi-faceted process for biometric verification

- ✓ **Face Matching:** Confirms the person on the document is the same on the video or selfie.
- ✓ **Audio Processing:** Verifies digits by processing voice to text.
- ✓ **Face Tracking:** Tracks specific, verifiable facial motions to verify head turn, and checks for 3D face consistency.
- ✓ **Mouth Tracking:** Tracks lip movements to ensure that they match the voice.
- ✓ **Texture Analysis:** Finds and analyzes videos of screens for texture.
- ✓ **Expert Review:** When the machine can’t reach a conclusion, humans analyze all available information.

Deep dive: Hybrid approach to fraud detection

Onfido uses a hybrid approach to provide the level of confidence you need for high-value transactions.

Our process:

Sample the video at a high frame rate, and compare all the frames to the face on the document. We make sure all the frames show the same person throughout the whole video – no swapping of identity partway through.

Extract the audio from the video. Use speech-to-text technology to compare what the user with the actual instructions of what they were asked to say.

Track the face during the video to confirm two things: 1) Is the face 3D consistent? For instance, does the nose protrude, do the eyes sink in, and does the face turn in the direction that was asked? 2) Are the lips moving when sound comes out of them?

Analyze texture in a similar way we analyze selfies, on multiple video frames, to make sure there’s always a real human face on the screen. Our goal is to eliminate the possibility of print-outs or digital screens.

If any of our algorithms detects the possibility of fraud, we escalate to our expert reviewers, resulting in the most accurate face matching and spoofing detection possible.

Digital identity verification requires a rigorous approach

Fraud detection technologies are making strides—but they don't work in isolation. Defeating sophisticated types of digital identity theft requires the ability to quickly and accurately use biometric methods when needed.

Onfido is the only solution provider that uses a hybrid approach. We analyze a range of signals from personal data, biometrics, and IDs to determine whether someone is the person they claim to be.

Lower your fraud exposure risk with Onfido

- Our platform uses global IDs as a primary source of identity and compares them to a digital capture of the user in either a photo or a video.
- Combined with our unique approach to biometrics, we deliver better results than machine-learning solutions or humans alone can achieve.

But does it scale?

Onfido combines the best of automated and manual verification in a robust, scalable platform designed for the needs of today's digital companies. Built to meet global regulations, it allows you to stay in compliance with global data privacy laws, sovereignty restrictions, and customer due diligence regulations.

> A car rental marketplace saw a 22% decrease in theft attempts after they switched to Onfido from a competitor.

Solve the toughest challenges in ID verification

Any business with a digital component needs to have a solution for verifying identify—ideally, one that is easy to use, highly accurate, and cost-effective. Onfido delivers on all that and more, so that you can welcome legitimate customers and keep the imposters out.

Grow with confidence.

With a reliable hybrid solution for IDV, you can onboard more users and build trust in your business.

Provide a great user experience.

Many fraud detection methods can be unfriendly to users, causing them to give up and abandon the task or transaction. Onfido provides a simple, accessible customer experience and reduces service calls.

Save money.

In addition to preventing costly fraud, Onfido is affordable to operate, delivering better value than manual solutions or expensive, hard-to-maintain on-premises software.

Learn more about the Onfido difference

Find out more about Onfido's fraud detection solutions.

Learn More

Try the Onfido demo app:

Download on App Store

Download on Google Play

onfido

Sources:

1 Sourced from NIST: National Institute of Standards and Technology, a physical sciences laboratory, and a non-regulatory agency of the United States Department of Commerce