

The Inevitable Collision of

# IDENTITY PROOFING & AUTHENTICATION



jumio®

# ONCE UPON A TIME, THE INTERNET WAS A MORE ANONYMOUS SPACE.

No one likes having their online movements tracked. But, advertisers routinely track our internet habits across our devices — phone, tablet, laptop — to know where we habitually go, shop, and what kind of websites we visit. Worse still is having those advertisers profit from that information when they sell it to third parties without our consent.

The other side of the anonymity coin.

Online businesses increasingly need to know who they're dealing with online. Are the people creating new accounts who they claim to be? Is the person transferring \$10,000 to a Swiss bank account who she claims to be? As services, commerce, communications and socializing shift online, identifying each other digitally has become increasingly important.

In some cases, businesses are required to know the real person behind an account. Know Your Customer (KYC) is the process of a business verifying the identity of its clients and assessing potential risks of illegal intentions for the business relationship. KYC is also used to refer to the bank regulations and anti-money laundering regulations which govern these activities. KYC processes are employed by companies of all sizes for the purpose of ensuring their proposed agents, consultants or distributors are anti-bribery compliant. Banks, insurers and export creditors increasingly demand that customers provide detailed anti-corruption due diligence information.

But the internet's level of openness means the barrier to entry on a wide variety of online platforms isn't just low for users, but for bots and bad actors as well.

Most website visitors aren't humans, but are instead bots — or, programs built to do automated tasks. They are the worker bees of the internet, and also the henchmen.



Overall, bots — good and bad —  
are responsible for

**52% OF WEB TRAFFIC.**

*Imperva Incapsula Bot Traffic Report, January 2017*

The bots used to spread fake news are usually bad, and bad bots make up roughly 28 percent of internet traffic. Fake accounts have recently made headlines for maliciously influencing discourse on social media. However, bad actors also use fake accounts to commit financially motivated attacks, including reward abuse on retail sites, money laundering via online banking, and even as a disguise for credential stuffing.

### Data breaches make things even worse.

Just think of the scale of the breaches we've endured over the last few years: Yahoo!, Facebook, Equifax and Marriott's Starwood properties. These massive data breaches don't just impact the consumers whose username and password credentials are stolen — they impact the larger ecosystem and eviscerate the notion of online trust. When those breached records end up on the dark web, cybercriminals purchase the information and unleash a wave of fraud. They create new online accounts, reset passwords, initiate wire transfers and perform account takeovers — inflicting a lot of damage, financial loss and headaches. In fact, a recent report published by cybersecurity firm Shape Security showed that 80 to 90 percent of attempts to log into a retailer's e-commerce site are hackers using stolen data.

# 80-90%

of attempts to log into  
a retailer's e-commerce  
site are hackers using  
stolen data.

*Shape Security*



# TWO TYPES OF IDENTITY VERIFICATION REQUIRED: IDENTITY PROOFING AND AUTHENTICATION

The ability to reliably identify people online — and confirming that information against their “real” selves — is becoming increasingly important. Verification is now required by a surprising number of digital businesses, from purchasing products and applying for services, to social networking platforms, where users’ authenticity is built into the experience.

But there are really two types of identity verification involved — identity proofing and authentication. So, let’s start by defining the terms and understanding the differences.



## What is identity proofing?

Identity proofing is the process an organization uses to collect and verify information about a person for the purpose of opening an account or issuing credentials (i.e. username and password) to that person.

This typically involves three distinct steps: collection (capture evidence of identity), validation (confirm identity exists) and corroboration (ensure the digital identity belongs to a person).

Simply requiring a government-issued ID, such as a UK driver’s license, does not mean that the person presenting the ID is the actual owner of the ID. This is why a selfie is often required as part of the identity proofing process to corroborate that the person holding the ID document is the same person behind the online transaction. Identity proofing is usually the first step in establishing your online account or profile.



## What is authentication?

The technology research firm, Gartner, defines user authentication as “the real-time corroboration (with an implied or notional confidence or level of trust) of a person’s claim to an identity previously established to enable their access to an electronic or digital asset.” Put simply, authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be.

Identity proofing and authentication are commonly used as a two-step process, but they are distinct activities. Identity proofing is the process of verifying a claimed digital identity (usually when an online account or profile is being created) to ensure that it belongs to a real person. Once the identity proofing process is complete, users will often need to authenticate themselves to access an account, reset a password or perform a high-risk transaction (e.g., a wire transfer).



# IDENTITY PROOFING METHODS

More recently, enterprises are starting to require that new online customers capture a picture of their government-issued ID (drivers license, passport or ID card) and a selfie with their smartphone or webcam, and then compare the face in the selfie to the picture on the ID.

Let's explore some of these more popular methods of identity proofing being used today. For larger financial institutions, a variety of identity proofing solutions may be used together to better corroborate a consumer's true digital identity.



## Financial and Credit Bureau Lookups

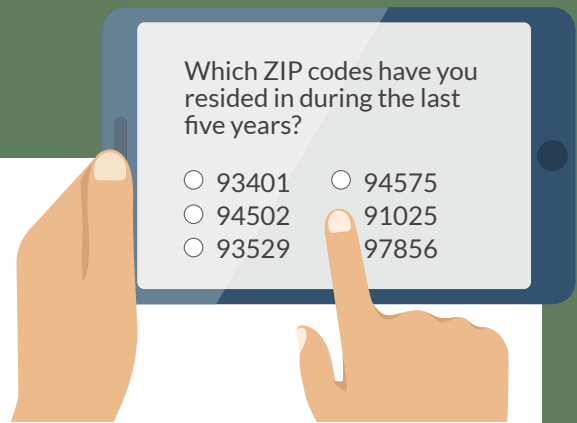
Historically, the function of “identity proofing” was based on the premise that if a person was able to provide a name, address, date of birth and a government identifier (e.g., Social Security number), he or she must be that person. Many online identity verification systems assess the identity of an individual by calling out to one of the big three credit bureaus (Experian, Equifax and TransUnion) who then search for an identity match within their vast repositories of consumer information.

These methods were never very sound given the significant amounts of personal data available on the dark web, but were deemed good enough. In addition, these solutions have proven to be relatively ineffective at detecting both synthetic identity and identity theft and are also weak at verifying the digital identities of individuals with limited credit histories due to age, the use of alternative financial services or recent immigration to the country whose records are being interrogated.

## Knowledge-Based Verification

This type of identity proofing and corroboration relies on public records for real-world activity and on credit bureau data to confirm or deny that the information provided by an individual matches the information on record. Typically, the user is asked several proofing multiple-choice questions such as “Which of the following ZIP codes have you resided in during the last five years?” and those answers are then corroborated against public records databases. Questions are often created on the fly based on the user’s public records or financial records history. Several data aggregators offer services for an out-of-wallet quiz and generate questions for an end user dynamically. Answers to these questions are difficult for a fraudster to guess since they are based on a user’s personal history.

Knowledge-based verification has proven problematic as legitimate customers frequently failed these questions, and it introduced a high rate of friction and abandonment. This method has also become ineffective due to the large troves of personally identifiable information (PII) captured by criminals in several security breaches over the last few years, and the large amounts of PII that can be found volunteered by users on social networks.



## Government-Issued IDs + Selfie



There's an emerging method of identity proofing as a service which relies on a photo of a passport, driver's license or other form of identification through a webcam or smartphone camera. The ID is then assessed for signs of tampering or counterfeit, and then the photo of the ID is compared to a selfie (still photo or short video) taken by the individual submitting the document. Most vendors in this space rely on artificial intelligence, machine learning and human review to assess the legitimacy of the ID document and selfie. Several vendors in this space hoist the manual review responsibilities on the business customers, while others perform this review themselves with suspect IDs.

# POPULAR AUTHENTICATION METHODS

After the customer has been vetted via one of the aforementioned remote identity proofing methodologies, that same customer usually does not have to go through the process again. Instead the customer can now use credentials (i.e., username and password) that were set up during the account opening to access the account or perform certain actions. The verification of those credentials is what we call authentication.

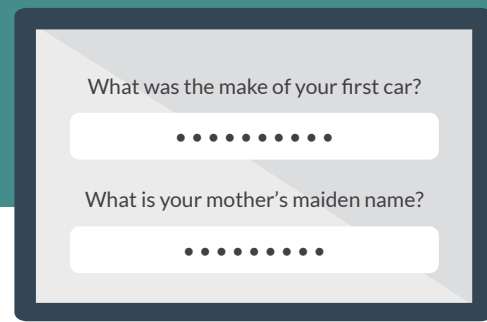
Authentication can include any number of methods, including password-based logins, knowledge-based authentication, hardware and software tokens, two-factor authentication and biometrics. Let's explore each in turn.

## Password-Based Logins

Amongst today's methods of authentication, the old-fashioned technique that requires a username and password remains the prevailing measure of securing computers, email accounts or online transactions. Unfortunately, passwords are inherently insecure.

Cybercriminals are routinely hacking into pretty massive databases where they're making off with millions of records at a time. The stolen credentials are often posted to the dark web where hackers can exploit them for identity theft and account takeover. Making matters worse, passwords are routinely forgotten causing many users to recycle the same password across multiple sites. So, when a hacker steals a person's password, they can often use it to access other online accounts which magnifies the impact and the damage.



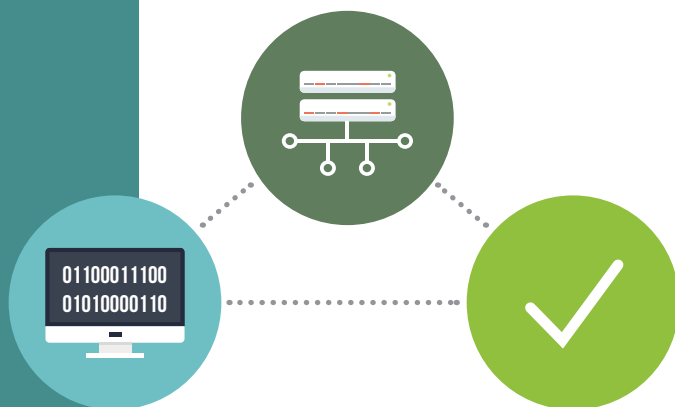


## Knowledge-Based Authentication

With traditional knowledge-based authentication, verification information is collected from the end user and presented in a future challenge/response authentication session on demand. Examples of this technique are security questions such as, “What is your mother’s maiden name?” The response to such questions is stored securely and recalled at a later date to verify an end user’s identity. However, this method is still susceptible to breaches if the data sources themselves are infiltrated or get compromised. Thanks to the dark web and social media, the answers to these “secret” questions can easily be discovered with a minimal level of effort by a determined fraudster who can then use that information to impersonate an individual.

## Token-Based Authentication

A token is a material device that is used to access secure systems. Common forms include a dongle, card, key fob or RFID chip. A token makes it more difficult for a hacker to access an account since they must have long credentials and the tangible device itself, which is much harder for a hacker to obtain. Hardware tokens have a number of challenges: they’re relatively expensive, easy to lose, and their administration and maintenance often take a heavy toll on IT departments. They’re also vulnerable to theft, breach of codes and man-in-the-middle attacks. Because of these shortcomings, software tokens have become more popular.

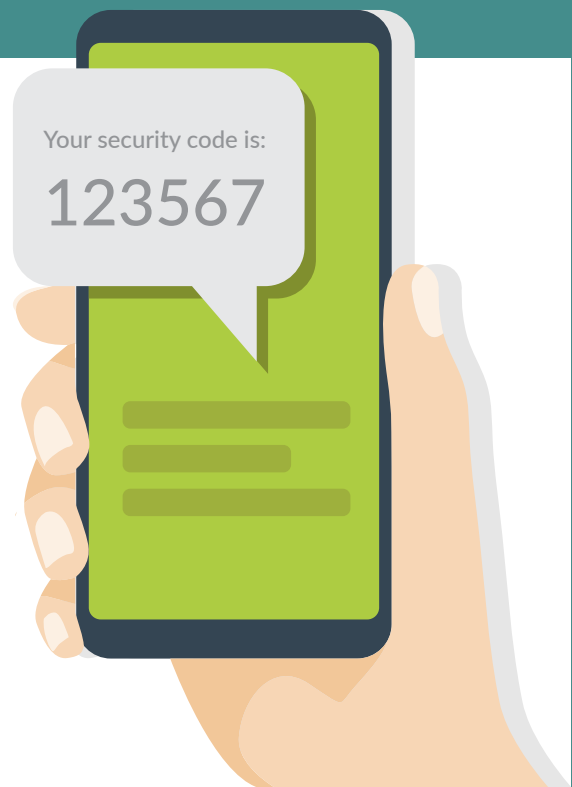


Instead of carrying around an extra piece of hardware, software tokens have been incorporated into smartphones (usually in the form of an app) or stored on a general-purpose electronic device such as a desktop computer or laptop. Software tokens have a number of advantages over hardware tokens — for example, they can be automatically updated and they can be distributed to users instantly, anywhere in the world — but they’re not perfect. These one-time passwords are non-transferable, which can be problematic if a phone is lost, stolen or replaced.



## Out-of-Band Authentication

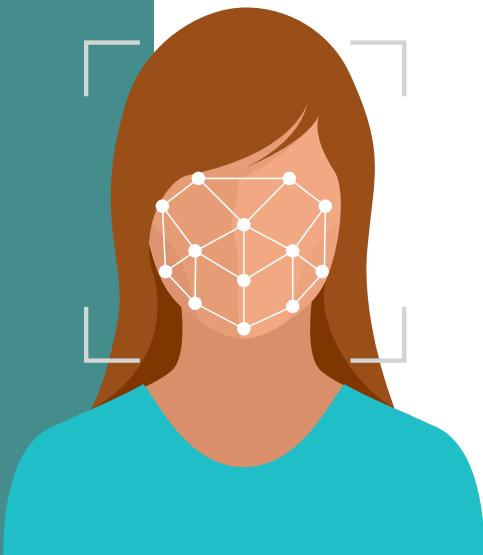
Out-of-band authentication is a term for a process where authentication requires two different signals from two different networks or channels. SMS-based out-of-band authentication is among the most popular methods in this category. With this type of authentication, a one-time security text or password is sent by SMS (text message) to the user. While this out-of-band technique is more secure than simple password authentication it is no longer recommended by NIST because of several vulnerabilities, including being susceptible to man-in-the-middle and snooping attacks, phishing and complicit user fraud.



## Biometric Authentication


Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who he says he is. Biometric authentication systems compare biometric data captured at the time of login to confirmed authentic data stored in a database.

The important thing to note is that the match between the two data sets has to be nearly identical but not exactly identical. This is because it's impossible for biometric data to match 100 percent. Juniper Research forecasts that users of these methods will increase from an estimated 429 million in 2018 to over 1.5 billion in 2023 (source: Mobile Payment Security: Biometric Authentication & Tokenisation 2018-2023).



# STEP-UP AUTHENTICATION

Many of the aforementioned authentication methods are triggered for potentially high-risk transactions. Step-up authentication is when a user is challenged to produce an additional form of authentication. When the business logic determines that there is need for an additional form of authentication (because of inherent risk), then it triggers a step-up authentication based on a variety of risk factors, including:

- 
- ✓ Logging in from a foreign IP address
  - ✓ Password resets (to try to prevent account takeovers)
  - ✓ Large money or wire transfers
  - ✓ Multiple unsuccessful logins
  - ✓ Requested change on authorized permissions
  - ✓ Door opening (car rentals, hotels, home sharing services)



## FRAUD DETECTION

Best practices suggest that organizations adopt a layered approach to fraud prevention techniques for their internal systems to compensate for weaknesses inherent in using only authentication methods. The fact is, no single layer of fraud prevention or authentication is enough to keep determined fraudsters out of enterprise systems.

That's why more and more organizations are layering in technologies to sniff out potential fraud signals. By capturing a fixed set of personal device (e.g., smartphone, laptop, etc.) attributes — browser configuration, operating system, IP address, wireless settings, screen resolution and more — device-based fingerprinting can identify computers and mobile devices used to commit fraud, so your company can avoid becoming the next victim.

Another approach to fraud detection that's gaining some market traction is behavioral biometrics. Behavioral biometrics is based on the creation of a unique profile for every customer (e.g., based on keystrokes, swipe gestures, mouse movements, etc.). This profile is further augmented with device-based data and third-party data sources to better distinguish between legitimate customers and fraudsters. This class of solutions gathers human biometric patterns to identify fraudsters or bots trying to impersonate legitimate users when creating new accounts.

They do this through a variety of methods such as detecting anomalies in mouse acceleration or by identifying suspicious keyboard velocity. In some cases, they're looking for above-average fluency with a site or keyboard shortcuts and function keys (not possessed by the average consumer). For example, fraudsters using these advanced skills will complete an online application in seconds whereas the average user takes minutes to complete.

## COMPARING THE DIFFERENT METHODS

Historically, enterprises have to balance three variables when it comes to identity proofing and user authentication: identity assurance, ease of use and fraud detection.



### Identity Assurance

How certain are you that the person behind the account set-up and login is who they claim to be? Many of the aforementioned methods don't really provide much identity assurance. Thanks to large-scale data breaches, identity theft, phishing and social engineering, businesses can't trust that someone is who they claim to be, even if they have their mailing address or possess the correct Social Security number.



### Ease of Use










How simple are the online identity proofing and authentication processes? Increasingly, consumers are demanding a rapid, low-friction experience that makes security invisible. According to a 2016 Signicat Survey, 40 percent of online bank account applications were abandoned due to a long or complicated enrollment (i.e., identity proofing) process.


















### Fraud Detection

How well can the solution detect malware, bots and bad actors? Companies need to be able to confidently assess risk and make more informed application-processing decisions while minimizing fraud loss. Companies also need to better detect identity theft, account takeover and synthetic fraud — some of the largest threats facing online organizations today.

Companies are adopting and investing in the technologies that make security invisible to their customers, but also result in higher conversion rates as well as higher rates of fraud detection. The table below provides a quick comparison of the different identity proofing and authentication methods along these three dimensions:

Identity Proofing			
Method	Identity Assurance	Ease of Use	Fraud Detection
Financial & Credit Bureau Lookups			
Knowledge-Based Verification			
Government Issued IDs + Selfie			

Authentication			
Method	Identity Assurance	Ease of Use	Fraud Detection
Password-Based Logins			
Knowledge-Based Authentication			
Token-Based Authentication			
Out-of-Band Authentication			
Biometric Authentication			

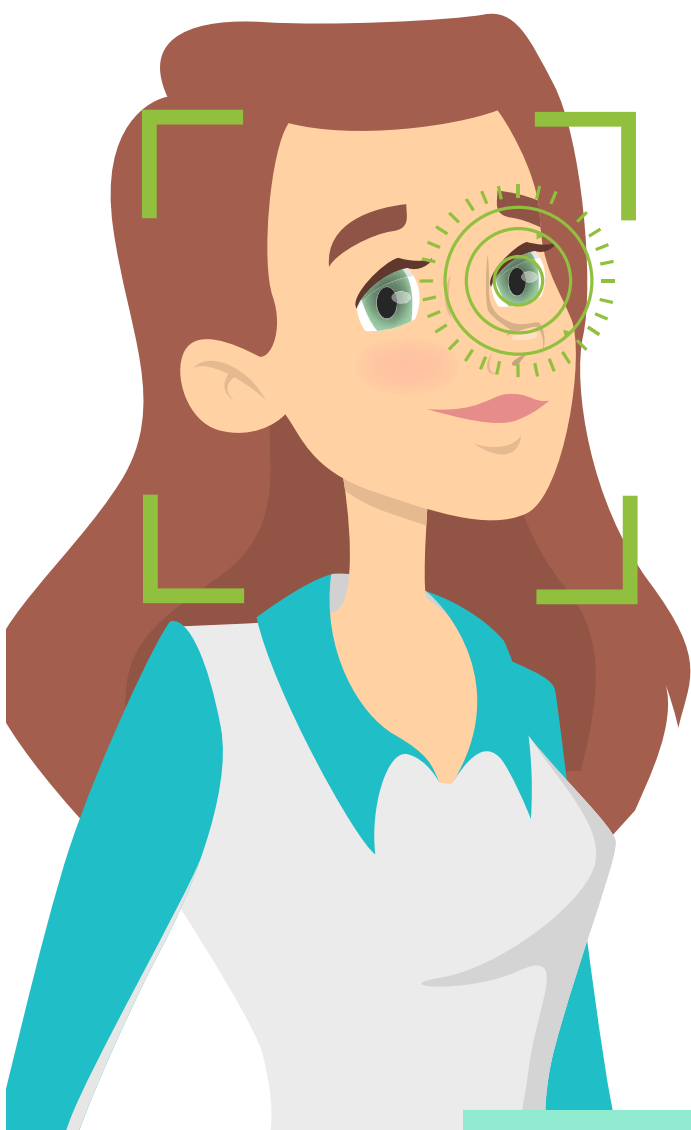
# THE IMPORTANCE OF LIVENESS DETECTION

As biometric-based verification has grown in popularity, the incentives for fraudsters to penetrate the systems have grown as well. Now known as “spoofing,” lifelike artifacts are used as a means of tricking the biometric systems into creating new online accounts by falsely accepting an artifact in lieu of a real person. Spoofing attacks vary depending on the biometric modality, with common examples being photos, video playback, masks, voice recordings or even just voice impersonations.

The reality is our biometric data is everywhere — just think of the cloud-stored photos, YouTube videos and Facebook accounts online already. Our fingerprints are on everything we touch and we have all heard “This call is being recorded for quality assurance purposes.” On top of that, more nefarious sources also sell this data to fraudsters, with multiple dark web sites offering account credentials with user selfies. That is why any identity verification solution based on biometrics must have robust anti-spoofing measures in place.

Liveness detection protects a system from unauthorized access by spoofing attacks by ensuring that the images are captured from a real human and not a spoofing artifact. True real-time liveness detection is absolutely critical for the security of biometric systems, whether it is for user identity authentication for login or remote onboarding and enrollment.

Until recently, there has not been a NIST-certified third-party test guided by the International Organization for Standardization (ISO) presentation attack detection (PAD) standard that can verify the abilities of liveness detection vendors to detect and repel spoofing attacks. For years this lack of oversight allowed biometric vendors to exaggerate their security claims and resulted in a false sense of security that many criminals took advantage of. Thankfully, objective spoof detection testing from iBeta/NIST is now in place and today’s technology providers can be comprehensively evaluated, bringing much-needed transparency to the industry.



# WHAT IS THE ISO 30107 PAD STANDARD?

The ISO/IEC 30107 is an evolving spec that provides testing labs a technical foundation for PAD tests by defining terms and establishing a framework through which presentation attack attempts can be categorized, detailed and communicated for subsequent decision-making and performance assessments.

The goal of PAD is to determine if biometric data is a first-generation acquisition from a live person present at the time of capture, or if it is from an artifact designed to emulate the traits of a living 3D person. In addition, the ISO standard also considers the availability of the original biometric data and rightly requires test subjects be fully cooperative and provide any and all biometric data requested by the testers. This ensures that the tests emulate both phishing and complicit user fraud scenarios as well.

The ISO/IEC 30107 standard as tested by iBeta considers three levels of spoof artifact:

Level 1	Level 2	Level 3
This includes the ability to detect 2D paper photos (flat and bent), digital photos and videos exhibiting blinking and 3D motion, paper masks (flat and bent) with eye and mouth holes cut out and worn by a real human	Ability to detect 3D lifelike dolls, mannequin heads and realistic masks that can be purchased for under \$300 and worn by a real human	Ability to detect Hollywood-quality 3D latex and silicone masks, hyper-realistic wax figures and high-quality 3D printed faces with professional makeup

To put the difficulty of these tests in perspective, Apple's specialized infrared camera hardware for Face ID has been spoofed by a Level 1 artifact.

Even though many face verification software solutions have aimed to solve the spoofing problem in the past, none have been able to effectively pass third-party presentation attack testing, and therefore can't be taken seriously by the market. Solutions from vendors making liveness detection claims that can't be backed up by third-party testing have no place in the biometric security market.

Making certified liveness detection a key part of your biometric verification process ensures a safe and secure experience for your user, enhances trust in your brand and paves the way for improved business-client exchange and relations.



# THE INEVITABLE COLLISION OF IDENTITY PROOFING AND AUTHENTICATION

What's interesting about the previously outlined methods is how they're largely mutually exclusive options with little overlap between the methods of identity proofing and authentication. That's why so many organizations use one method for identity proofing and another for authentication.



But, the lines are blurring between identity proofing and authentication thanks to advancements in biometrics and broad-based familiarity of using one's face as a second factor. Increasingly, the biometric that is gaining the most adoption has been the face. Face ID is now the sole means of biometric authentication on Apple's iPhones, and it looks like the company will stick with this system for the foreseeable future. All of Apple's new mobile devices have abandoned Touch ID fingerprint authentication in favor of Face ID, an infrared, 3D face authentication system.

Because Apple is so ubiquitous, they've essentially brought Face ID to the masses, fostering the widespread adoption of face-based biometric authentication.



## A MORE PERFECT UNION

If the goal is to leverage the biometric data captured during enrollment and reuse it for future user authentications, then there's an extra step that must be addressed when the biometric data is captured — performing a liveness check to ensure that it's a real person performing the transaction.

When we discussed using a government-issued ID along with a selfie, we had not yet discussed the importance of liveness detection. But, if enterprises are going to rely on a driver's license and a selfie, they need to also perform liveness testing on the selfie in order to ensure that the person behind the initial enrollment is physically present.

Identity verification providers, such as Jumio, have embedded 3D liveness detection into the identity proofing process to better thwart fraudsters who are increasingly using spoofing attacks by using a photo, video or a different substitute for an authorized person's face to acquire someone else's privileges or access rights. A 3D face map is created based on up to 100 frames (images) from the smartphone.

In addition to checking the authenticity of the ID document and ensuring that the image in the selfie matches the person pictured on the ID, Jumio is ensuring that the new customer is physically present without relying on any special hardware in the phone itself. As part of the identity proofing process, liveness detection algorithms analyze biometric data (images) from the smartphone's front-facing selfie camera or your computer's webcam. Jumio creates a 3D face map of the user, which is then stored and bound to the new customer's identity during the initial enrollment process.

While the identity proofing and liveness detection processes may take a minute or two, they provide business customers with a high level of identity assurance and save users time in the future as they can use their selfie to instantly prove their identity. This is what Gartner refers to as an “identity corroboration hub.”



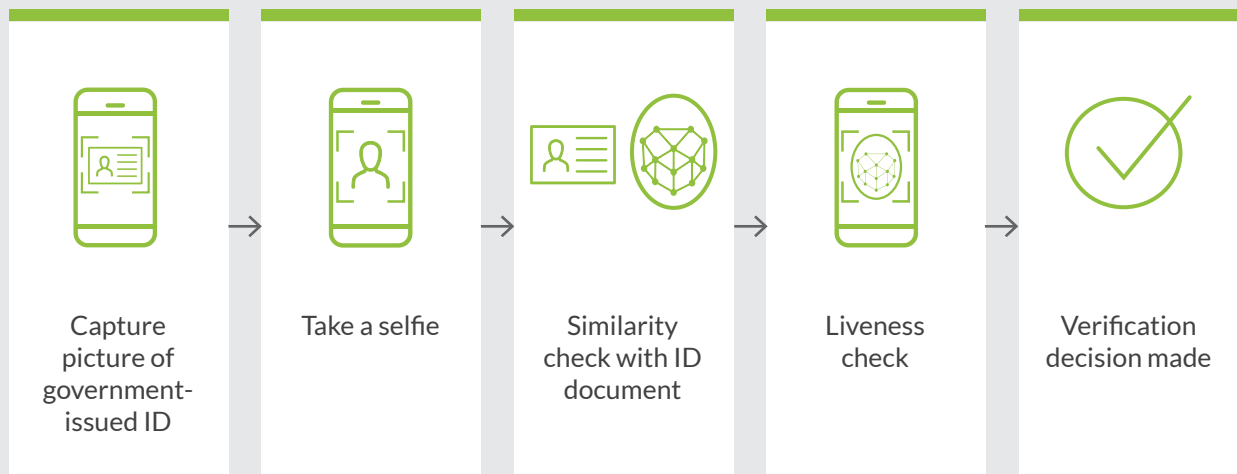
**“By 2023, identity corroboration hubs will displace existing authentication platforms in over 50% of large and global enterprises.”**

**Gartner®**

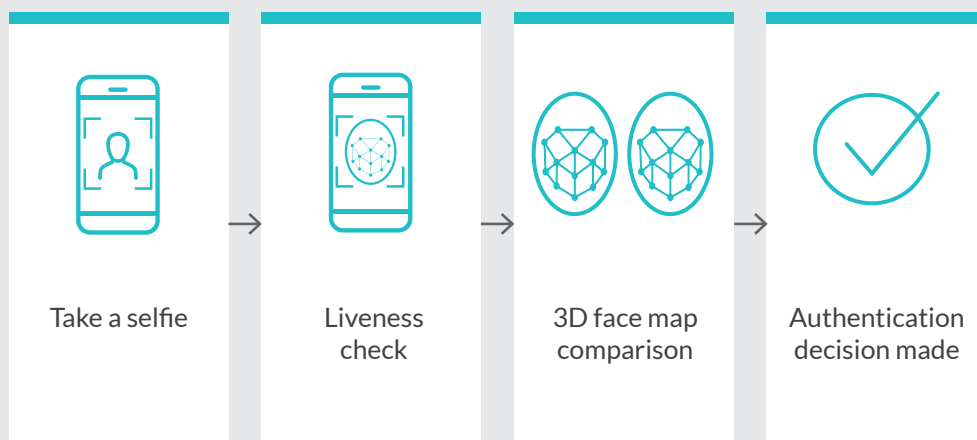
Once the corroboration hub is in place the real benefit of storing a trusted 3D face map at enrollment is realized. During a future user authentication, a new selfie is taken and a new 3D face map is created. This face map is then compared with the trusted face map stored from the initial enrollment and a match/no match decision is made in seconds.

The elegance of this solution is that the user is never again required to complete the identity proofing process — they just need to take a new selfie.

## Identity Proofing Steps



## Authentication Steps



By using a selfie to create a 3D face map during enrollment and then authenticating users with a new selfie each time they make a significant transaction, organizations will realize a number of tangible benefits, including:



### Identity Assurance

By requiring a valid government-issued ID and matching it to a selfie (with embedded 3D liveness detection), enterprises can have a much higher level of assurance that the person is who they claim to be.



### Ease of Use

Thanks to the popularity of Apple's Face ID, face-based authentication has become more familiar and accepted. When combined with certified anti-spoofing capabilities, biometric-based authentication improves the user experience and reduces friction because of its ease of use, speed and omnichannel support (across mobile devices and webcams).



### Fraud Detection

Certified liveness detection provides an additional layer of fraud prevention for digital businesses during the account creation and authentication processes. Strong liveness detection solutions thwart fraudsters who are increasingly using spoofing attacks to acquire someone else's privileges or access rights. Perhaps, more fundamentally, requiring a selfie is a huge deterrent because fraudsters don't want their real face captured by the company they're attempting to defraud.



# TODAY'S USE CASES: UNLOCKING YOUR DIGITAL IDENTITY

By adopting your users' selfies as their second authentication factor, organizations can now envision new use cases that go well beyond suspicious logins.



## Secondary authentication

Instead of (or in addition to) using username and password, organizations can use the selfie as a second-factor authentication.



## Authorize high-risk actions

Authenticates users prior to high-value transactions like wire transfers, online purchases or bill pay. By requiring a selfie, financial institutions and their online customers can rest assured that the request is legitimate and has been authorized.



## Unlock doors

An end-user has made a car rental reservation, and the selfie is used to unlock the car.



## Self check-in

The end-user can use his or her face for self check-in at hotels or to check in for a flight eliminating the need to wait in long lines.



## Update user credentials

Every use case in which authentication is required — logins, forgot/reset passwords, update phone numbers and addresses, etc.



## Continuous security

Regular authentication requested from the end user, for instance to ensure no account takeover happened.



## E-learning

Universities, e-learning providers and proctoring services often need a reliable solution to ensure a student who wants to take an exam is really the individual who is expected to complete that test. The end user is requested to authenticate before and even during the exam.

# THE DEATH OF PASSWORDS, MAYBE.

At the same time, more and more consumers are using their mobile devices to create new online accounts and to access those accounts and online services on the go. Given these parallel trends, it's not surprising that face biometrics are now taking the place of fingerprints, PINs and passwords, with Apple's Face ID paving the way. Face-based logins from Apple and Samsung are prompting other manufacturers to include the feature in their devices. Estimates by [Counterpoint Research](#) suggest that more than one billion smartphones will have some form of a face unlock solution in 2020.

So, the good news is that more and more users are getting comfortable unlocking their phones using their face. Unfortunately, in many cases, users don't just need a better way to unlock their devices — they need a real way to prove their identities online. These new hardware biometric face scanners give users a false sense of security when it comes to identity assurance.

Here's why:

Hardware-based biometrics are tokens and they just say “yes” or “no” to an on-device matching request. These tokens don't say “This is Kevin,” as they cannot prove the actual identity of the user. When a person gets a new phone, he or she must re-enroll their face print because all of their historic biometric data was stored on their old device. The user is required to re-enroll their face on the new device, but the new data that gets enrolled could be yours, your child's, your co-worker's or a criminal's. Sadly, the on-device sensors do not know the difference.

In order to realize the promise of face-based authentication and reduce our dependence on passwords, several ingredients need to be in place, including:



## Reliable Identity Proofing

Before any credentials are disseminated, businesses must have a high level of assurance that the customers are who they claim to be. Traditional methods such as static data checks, don't prove that someone is actually who they claim to be. Pairing a valid government-issued ID with a selfie and 3D liveness detection provides a high level of identity assurance.



## Encrypted Storage of Trusted User Data

In order to enable reliable, biometric-based authentication, modern companies must be able to accurately compare new biometric data with the biometric reference data captured during enrollment. When using a selfie, it's imperative to build an individual's history of biometric information for comparison, which increases the odds of an accurate face map match.





## Customer Experience is Paramount

Regardless of the method of identity proofing and step-up authentication, there will be some friction involved. Solution providers must provide a simple, intuitive and familiar user experience that takes seconds to complete and involves just a few steps. Companies can't afford to lose viable prospects during the account set-up process because of a clunky user journey.



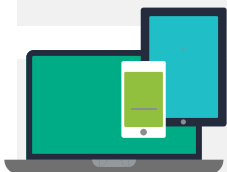
## The Role of Familiarity

It's difficult to overstate the importance of Apple's Face ID to widespread biometric adoption of consumers. Without this familiarity, companies would be hard-pressed to use a simple selfie as an authentication factor. Biometric solutions that lack this level of end-user familiarity have a much tougher road to hoe.



## The Need for Speed

While most users are willing to endure a bit of friction when creating an online account, they're increasingly demanding identity proofing and authentication solutions that are fast (performed in seconds) and reliable. Modern face-based authentication can now quickly compare a new selfie to a previously captured selfie with a very high level of identity assurance.



## Cross-Platform Portability

Since Jumio's 3D face maps can be created on almost any device with a camera, true cross-platform biometric authentication is now possible — users can enroll using a laptop webcam and authenticate later from a smartphone or tablet. This means it's now possible to use face authentication for everything from unlocking a car door to performing a secure password reset to accessing your bank account.

## CLOSING WORDS

As identity proofing and authentication processes converge, we think the role of face-based biometrics will enable broader adoption, provide higher levels of identity assurance, improve the customer experience and conversion rates, and better protect online accounts from identity theft and account takeover.

While we may be a few years away from killing the password altogether, we're starting to see the increased adoption of face-based authentication as a dominant way of unlocking our mobile devices. Next we'll see it unlocking our online accounts as solutions such as Jumio Authentication streamline the identity corroboration process by capturing and comparing 3D face maps across a wide variety of authentication use cases.

With biometric face authentication, consumers will have greater trust that their online accounts are protected against account takeover and online fraud. Modern businesses can better protect their ecosystems from bots, malware and cybercriminals by ensuring that their users have been vetted and that high-risk transactions have built-in safeguards.

The promise is undeniable. And the technology is here.

When identity proofing collides with strong, biometric-based authentication, we will fully unlock the power they both offer and take a big step toward a stronger global identity ecosystem.

## ABOUT JUMIO AUTHENTICATION

Jumio Authentication enables users to verify themselves during high-risk transactions and to unlock everything from online accounts to rental cars on any device.

The new solution is the first in the market to leverage biometrics for initial identity proofing and ongoing user authentication — creating an online experience that is fast, secure, accurate and easy to use.

This secure and rapid authentication method is ideal for account logins and high-risk scenarios (e.g., logging in from a foreign IP address or authorizing high-risk transactions such as wire transfers and online purchases). Secure selfie authentication can also be used to unlock doors (rental cars), self check-in (hotels), e-learning (online test taking) and continuous security (e.g., re-verifying the identity of ride-sharing drivers on a frequent basis).

# HOW JUMIO AUTHENTICATION WORKS

Biometric-based Jumio Authentication establishes the digital identities of your users through the simple act of taking a selfie. Advanced 3D face map technology quickly and securely authenticates users and unlocks their digital identities.



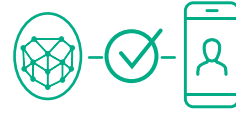
## 1. Acquisition

When a new online account is created, Jumio captures an image of a valid government-issued ID (driver's license, passport or ID card) and a 3D face map.



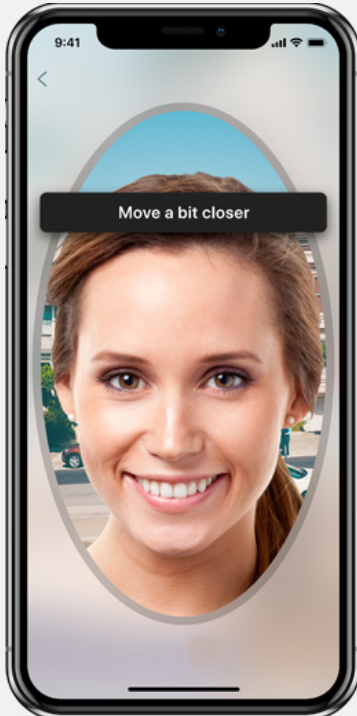
## 2. Comparison

A high-resolution selfie is compared to the photo on the ID to reliably establish the digital identity of the new user.



## 3. Authentication

When future user authentication is needed, Jumio Authentication captures a fresh 3D face map and compares it to the original face map to unlock the user's digital identity in seconds.



With Jumio Authentication, the digital chain of trust starts at enrollment when an online user takes a photo of their government-issued ID (driver's license, passport or ID card) and then takes a video-selfie, which is instantly analyzed via AI to determine that they are a living human and not a spoof. The selfie is compared to the picture on the ID document to reliably establish the digital identity of the new user.

Later when the user wants to log into their account or whenever a high-risk transaction occurs, Jumio Authentication allows the user to take another video-selfie (where a new 3D face map is created), which is then compared to the original face map, verifying the user and unlocking the account in seconds.

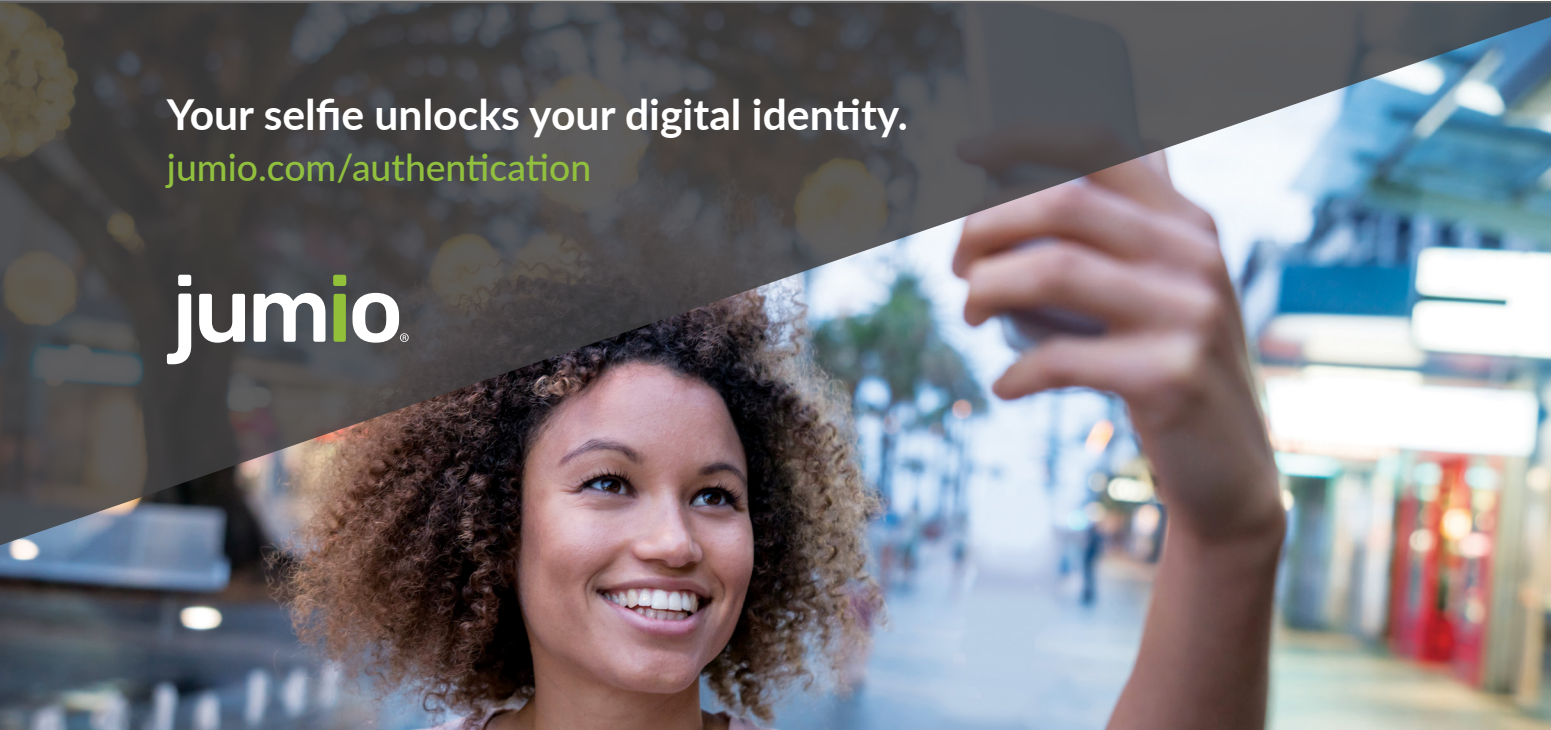
# ABOUT FACETEC

Jumio has partnered with FaceTec to integrate its ZoOm® 3D Face Liveness Detection to our online identity verification suite. ZoOm's capabilities improve the security, speed and user experience for liveness detection of new users, providing an additional layer of assurance and fraud prevention for digital businesses during the account creation process. This helps Jumio deliver a more definitive "yes" or "no" decision to our business customers on the identity verification transaction.

FaceTec's ZoOm 3D Face Authentication is the first — and only — biometric solution to achieve perfect Level 1 and Level 2 anti-spoofing results in NIST/NVLAP-certified iBeta Presentation Attack Detection (PAD) Testing. Following a 100% Level 1 anti-spoofing certification in August 2018, the rigorous Level 2 test validates the effectiveness of anti-spoofing Liveness Detection technology against realistic 3D artifacts and masks worn by living human testers. The iBeta PAD certification is the only test guided by the ISO 30107 global biometric testing standard.

Passing the Level 1 and Level 2 PAD tests required ZoOm to successfully stop more than 3,300 spoof attempts over 12 days of rigorous testing with sophisticated attacks using digital and paper photos, high-res video, lifelike dolls and realistic latex masks. No spoof attempts were able to fool the system and ZoOm achieved a perfect 100% anti-spoofing score over both tests.

This FaceTec integration translates into a better and more accurate experience that helps digital companies increase their confidence that new users are who they claim to be during the crucial new customer onboarding process. The upgraded liveness detection functionality provides a more seamless experience that helps convert more legitimate customers and better flags suspicious accounts who attempt to spoof the liveness detection process. These advanced liveness detection technologies provide Jumio a significant competitive advantage in terms of speed, accuracy and anti-spoofing capabilities.



Your selfie unlocks your digital identity.

[jumio.com/authentication](https://jumio.com/authentication)

**jumio**®