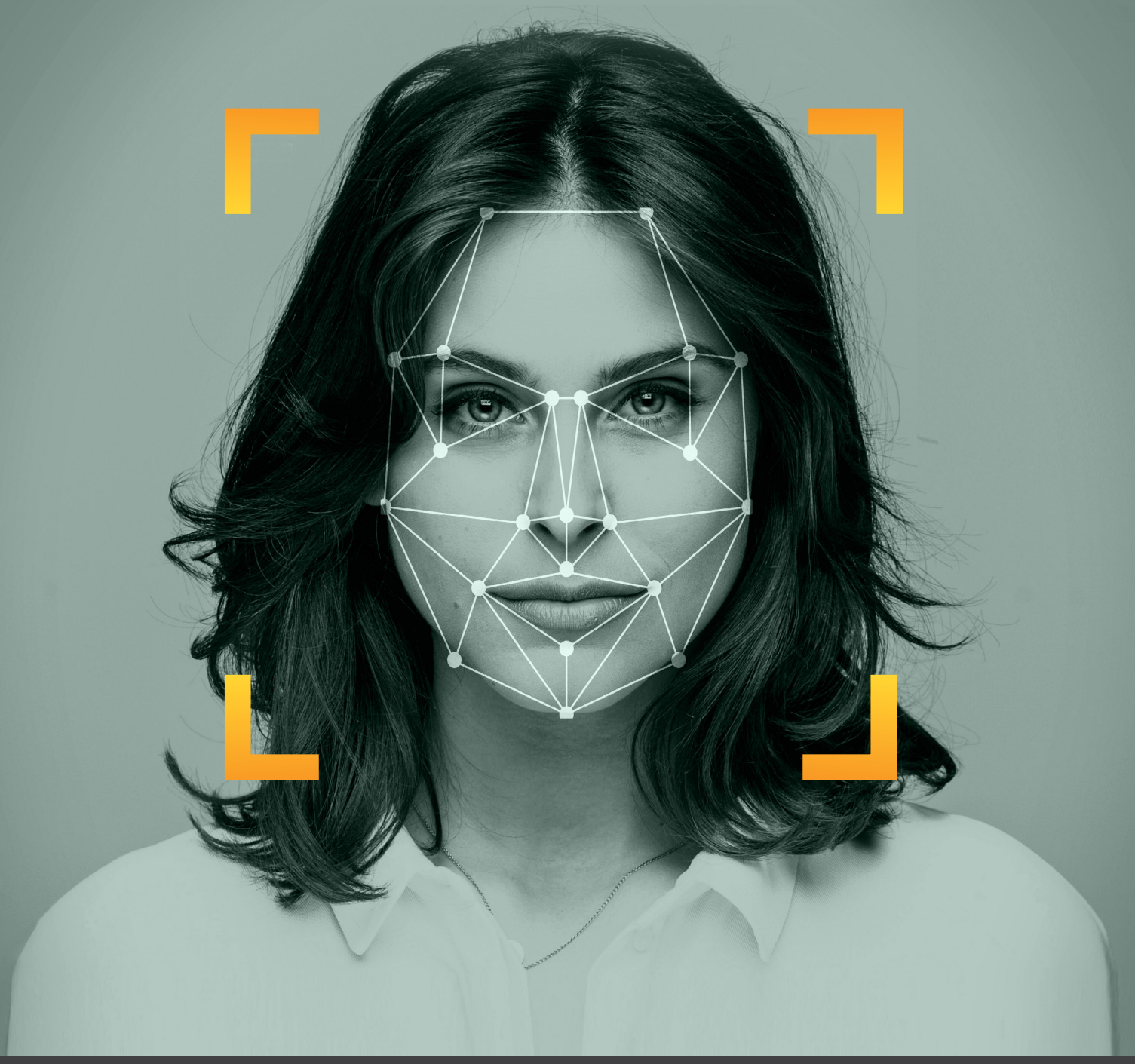
ENHANCING TRUST

with AI-Driven Biometrics



A FindBiometrics White Paper
Sponsored by Jumio and FaceTec

FINDBIOMETRICS
GLOBAL IDENTITY MANAGEMENT

jumio

facetec

BEING SMART ABOUT IDENTITY

Biometrics and AI Build the Strongest ID Verification Tech

Biometrics are commonplace. They protect our phones, log us into our virtual workspaces, secure our health records and verify our identity when we sign up for new services. Face, fingerprint, iris, voice and other modalities proliferate across our physical and digital lives, facilitating access, managing identity and keeping us safe from fraud. But it is crucial to understand that not all biometric technology is created equal.

The fact is, there are smart biometrics and basic ones. Functionally, all true biometrics, regardless of the modality, do what the name implies: measure unique physical or behavioral traits and compare them. Some consumer-grade biometric solutions keep it simple, measuring and comparing and matching the same way every time. On the other hand, smart biometrics, which are enhanced by artificial intelligence and machine learning, adapt with every use, getting stronger, faster and more scalable. The latter type is a foundational aspect of a broader trend that FindBiometrics calls “Intelligent ID” – a key technology for the future of our increasingly digital and mobile lives.

Artificial intelligence is a heavy term in our culture, and it brings with it a great deal of baggage in the form of common misconceptions. When it comes to intelligent biometric identity, these misconceptions pool around face biometrics, identity proofing and continuous authentication, which taken together are the basic components of a trust chain. Fears about user privacy, distrust stemming from racial bias reports in surveillance systems, and the expectation that identity proofing must rely on a human element in the onboarding process are all common false precepts clouding the understanding of smart biometrics in ID verification and user authentication.

Underneath that fog of misconception, AI-enabled biometrics offer revolutionary enhancements to the identity ecosystem. From creating a trust anchor, to image matching, authenticating and assessing user liveness, AI can effectively improve every aspect of the identity lifecycle while providing three broad benefits:

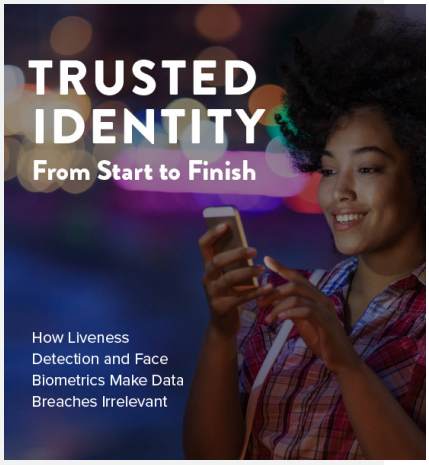
- AI enhances the speed, accuracy and scalability of identity verification and authentication.
- AI reduces the cost of identity verification and authentication.
- AI enables an identity verification and authentication system to flexibly respond to new and emerging fraud threats.

But the incorporation of smart biometrics into an identity verification and authentication solution is more than just a matter of enhancements. AI is a necessary tool in the fraud arms race, enabling modern enterprises to adapt to constantly evolving threats. In the absence of intelligent identity technology, we will see continued failure of the legacy security frameworks responsible for the historic data breaches that defined the past decade, while instances of fraud continue to rise. Without AI and liveness detection, fraudsters will learn to spoof, or fool, biometrics systems as easily as they crack passwords, and consumers will lose confidence in what was once hailed as strong authentication.

It's easy to see why AI-driven biometrics are necessary. But how do they fit into the process of creating a well-anchored, unbreakable trust chain?

Trusted Identity and Liveness Detection

This white paper builds on the ideas explored in "Trusted Identity From Start to Finish," which established the foundational concepts of identity verification via remote onboarding, continuous authentication and certified biometric liveness detection in relation to digital identity systems. Download it for free here.



AI AND TRUST ANCHORS

Artificial Intelligence is the Smart Way to Know Your Customer

The Basics of Identity Proofing
Building a trust anchor begins with identity proofing.

Step One: The user takes a picture of their ID document (front & back). The ID is checked for authenticity.

Step Two: User takes a corroborating selfie. The selfie is also checked for authenticity.

Step Three: During the selfie-taking process, the user goes through liveness detection.

Step Four: The picture in the selfie is compared to the image on the ID.

Step Five: A definitive yes or no is delivered regarding the user's claimed identity.

A trust chain begins with a strong anchor (e.g., a driver's license or passport). Without absolute assurance that a user is who they claim to be when they open an account or enroll in a service, any subsequent authentication is useless. That's why we need strong identity assurance in onboarding, especially as our society shifts to digital models that enable remote work, and access to finance, healthcare and education resources.

Facing the Facts

In theory, any biometric modality can be used to create a trust anchor, but one type of identification has emerged as the ideal solution for digital remote onboarding: face verification. Contactless, software-based, versatile and capable of matching the face in a selfie to the face in a government-issued ID document (e.g., driver's license, passport), face biometrics are the natural choice when it comes to maintaining trust throughout the entire identity lifecycle. As such, this document assumes the use of facial recognition when discussing identity verification, authentication and liveness detection.

As presented in our previous white paper, "Trusted Identity From Start to Finish," a trust anchor is established using government-issued identity documents, biometric face matching and certified liveness detection technologies. To open an account or enroll in a service, a user simply takes a picture of an ID document, then takes a selfie with their phone or webcam for corroboration. Using AI-enhanced biometrics with advanced liveness detection and document reading technology, genuine users are verified with government-grade ID proofing, establishing a foundation of the highest trust for any subsequent authentication.

As with all identity processes, artificial intelligence can greatly enhance the efficacy of digital onboarding.

Face-to-Document Matching

The bulk of the onboarding process is in the face and document matching process. Taking a selfie and photographing your identity document is the most involved process in the average mobile/online account registration process, and AI can improve it in ways that make onboarding more trustworthy and user-friendly.

AI aids in the face capture, the credential reading, and the biometric matching between the ID and the selfie. Artificial intelligence can respond to environmental factors like lighting, glare, blur and document condition, it can straighten out document images to help with optical character recognition (OCR), and it can account for discrepancies in age and appearance between the present day user and their ID photo. All of these factors, which generally present serious challenges to basic digital onboarding, are addressed with smart identity technologies.

Beyond the user-facing factors of digital onboarding, AI also facilitates accurate document reading in mobile enrollment, automatically classifying the document type and nationality while checking for indications of fraud. The ideal digital onboarding solution doesn't require a human element when it comes to checking the genuineness of a captured credential, but that scenario can only be achieved if the software can keep up with the constantly evolving cybercrime landscape. Artificial intelligence and machine learning help ID verification technologies constantly adapt to the rapidly evolving counterfeit and fraud landscape, honing their accuracy with every onboarding.

The Cost of Bad UX

Friction is the "F" word in user experience. Too much friction in onboarding and authentication leads to abandoned transactions and users giving up before signing up. According to a 2019 Signicat report nearly 40 percent of all financial services applications in Europe are left abandoned. That's why it's crucial that process-heavy user tasks like onboarding are fast, accurate and easy to perform every time. AI-driven biometrics enhance the trust, security and ease of use in identity transactions, cutting down on fraud and increasing customer satisfaction.

Liveness Checks in Onboarding

The technology foundation of any modern, effective identity technology is liveness detection. When creating a trust anchor, liveness ensures that the selfie required as part of the face-to-document match is in fact not that of an artefact like a mask, photo, video or high-resolution video. It determines if the user is alive and present by identifying dozens of live human attributes. Just as AI is integral in ensuring that counterfeit documents aren't used in onboarding, AI-powered liveness detection allows an ID verification solution to stay up to date in the ongoing arms race, ensuring they can detect even the most sophisticated presentation and spoofing attacks.

We create trust anchors as solid foundations for the subsequent authentications that follow enrollment, and AI aids in continuously fortifying every link in that trust chain.

AI AND CONTINUOUS AUTHENTICATION

Every Transaction is a Link in a Trust Chain

In a sense, onboarding is the most critical step in the customer's digital journey. It's here that a trust anchor must be established before any subsequent transactions can be done. But that doesn't mean that this is where the need for strong authentication ends. A chain is only as strong as its weakest link, and establishing a truly strong chain of security means employing strong authentication continuously throughout the customer relationship.

The Three Phases of Building a Trust Chain

Acquire: When a new online account is created, the identity verification solution captures an image of a valid government-issued ID and a 3D face map.

Compare: At enrollment, a high-resolution selfie is automatically compared to the photo on the ID to reliably establish the digital identity of the new user. This process is bolstered with AI-powered liveness and counterfeit detection technologies.

Authenticate: In subsequent user authentication, the identity proofing solution creates a fresh 3D face map and compares it to the original to verify the user's digital identity in seconds.

Not only does this protect the end user and the transacting organization, it also helps to ensure compliance with increasingly stringent regulatory requirements like Strong Customer Authentication in the European Union's Revised Directive on Payment Services (PSD2), which demands that online payments be authorized using multi-factor authentication.

This also protects the account against account takeovers which is increasingly important in the wake of recent, large-scale data breaches. In fact, the number of stolen and exposed credentials has risen 300 percent from 2018 as a result of more than 100,000 data breaches (source: Digital Shadows, July 2020).

Fortunately, cutting-edge AI is able to meet this need for continuous strong authentication without hindering the customer experience – and can actually make it better.

Biometrics Smarten Up

While many facial recognition systems can only operate effectively under relatively rigid angle and lighting conditions, there are now sophisticated, AI-driven technologies that actually *learn* the end user's face, rather than seek to match one static image with another. These algorithms can thereby recognize individuals whose superficial appearance has changed: they won't suddenly fail to recognize someone who has aged, grown a mustache or put on sunglasses. What's more, AI-empowered smart biometrics can authenticate individuals under various environmental and situational conditions that would normally hinder a human being's ability to be sure about who they're seeing.

Such AI systems can also take additional data into account beyond face biometrics – things like geolocation, device preferences, login frequency and other behavioral markers that are uniquely associated with a given user. Adding this to biometric recognition delivers greater certainty in the authentication process, while the detection of aberrant and unusual behavior can prompt the system to raise red flags as appropriate.

Complex AI Means a Simple UX

In addition to substantially boosting security, this all adds up to a dramatically improved experience for the end user, who can authenticate themselves using a simple selfie under a wide range of conditions. It doesn't require perfect lighting, or a rigidly precise face angle, and false negatives virtually fall to zero. It's a fast, simple process for the end user, but the certainty of the AI-driven authentication process under the hood ensures the highest security.

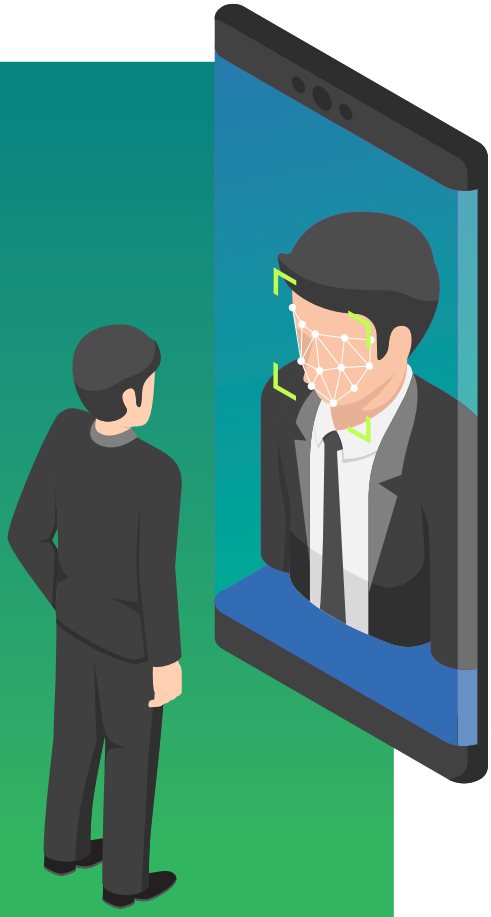
The Selfie Effect

Simply requiring a selfie with a liveness check can be enough to deter fraudsters, who generally succeed thanks to legacy ID proofing methods based on matching biographical data (name, address, SSN) to information held by credit bureaus. Biographical data is easy to obtain through phishing, and readily available for purchase on the black market. A selfie is harder to fake, and that extra obstacle can often mean the difference between a fraud attempt and a safe account. Jumio has found fraud attempts are reduced a staggering 90 percent simply by requiring a selfie with a liveness check as part of the authentication process.

AI AND LIVENESS DETECTION

Artificial Intelligence Will Win the War on Spoofing

The idea of "liveness detection" comes mainly from the world of fingerprint biometrics, where presentation attacks tended to be based on 2D images or material reconstructions of an authorized user's fingerprint, and thus presented a need to make sure that it was a real finger being used in the authentication process. In the world of face biometrics, liveness detection takes on an expanded meaning, referring to the ability to detect not only spoofing attempts using static 2D images, but also more sophisticated attacks like AI-generated deepfake videos.



Gimmick-Based Security

In an effort to add liveness detection to their authentication systems, some biometrics have implemented active prompts, like asking the end user to say a phrase or to blink while taking a selfie video. While these approaches introduce extra friction to the user experience, they can add a certain amount of security to the authentication session. But they can't detect the more sophisticated spoofing attacks that are emerging today. Realistic masks remain a threat in situations where fraudsters have the commitment to develop such tools, and there's also now the threat of video-based attacks that include AI-constructed deepfake videos that can create an uncanny likeness of a real person, starting with a simple 2D photo of another person, and make them do and say whatever the bad actors wish.

It's threats like these that make the development of anti-spoofing solutions into an AI arms race. Only sophisticated, AI-driven smart biometrics can detect the most advanced spoofing attacks, scanning for subtle clues of real end user liveness, such as the micromovements of hair, or the reflectiveness of skin; characteristics not present in spoof artefacts like videos. And the best of these AI systems are constantly evolving, training themselves to spot the latest threats as they emerge.

What's at Stake

Without incorporating this kind of AI technology, a liveness detection system runs the continual risk of becoming obsolete by advancements in spoofing technologies and strategies, even to the point where it can no longer be considered a true liveness detection solution. Meanwhile, relying on fundamentally insecure gimmicks that ask end users to perform additional actions during authentication can sacrifice the user experience and cause customer frustration, leading to increased abandonment.

Friction Versus Accessibility

In addition to slowing down the user experience, gimmick-based liveness detection can make ID verification and authentication downright inaccessible. Solutions that require a user to speak a passphrase assume the user can speak the language displayed by the app, that they are in an environment where speaking out loud is appropriate, and most importantly that they do not have a disability preventing them from reading or speaking. Identity should be all inclusive, and a frictionless biometric experience ensures ID verification and authentication is easy for everyone to use.

INTELLIGENT ID AND THE FUTURE

Secure, Convenient and Scalable – Digital Identity is Always Adapting

Just as the advent of digital access made the case for biometric authentication and ID verification evident, the increasing need for artificial intelligence in those same identity systems is now abundantly clear. Intelligent identity technologies comprising AI-enhanced biometrics and ID verification are available for deployment today, bringing with them greater speed, accuracy, security and a better overall user experience no matter the scenario in which they are deployed.

Already, we see AI-enhanced biometrics and digital onboarding playing a crucial role in a wide range of use cases.

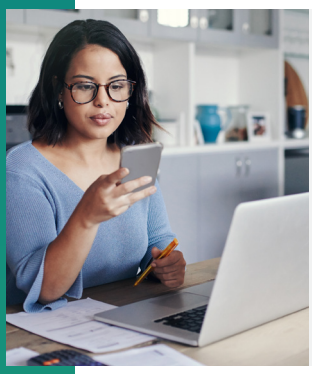
Use Cases: Intelligent ID Advantage

Banking and financial services:
Signing up for a bank account and conducting high-risk financial transactions remotely demands unimpeachable trust chains that can be built and maintained with ease and confidence. Mobility and digitization is making finance more inclusive around the world, and intelligent ID is keeping these services easy to access and fraud-free.

Transportation networks:
Rideshare and taxi services must be accountable for the identities of their drivers so customers can be safe when hitching a ride. With AI-enhanced onboarding, service providers can ensure drivers are who they claim to be and have a genuine, current driver's license, while subsequent smart authentication ensures only onboarded drivers are operating on-duty cars.

Digital wallets:
To protect your most valuable virtual assets – be they currency, credentials or health records – digital wallets demand the strongest trust chains possible. AI-enhanced ID verification, authentication and liveness detection means would-be thieves will walk away from a digital heist attempt empty-handed.

Remote work:
The COVID-19 pandemic accelerated the growing trend of remote work, and with an abundance of home offices comes an expanded cyberthreat attack surface for an enterprise. Intelligent ID technologies ensure employees can be onboarded and authenticated no matter where or when they clock in.



Education:
Online education is becoming commonplace, and it is crucial to know who is showing up to class, accessing records and taking exams. By having AI-enhanced biometrics and ID verification guarding digital classrooms and exam halls, institutions can ensure that their certifications and diplomas stay as trusted as their online security.

Account recovery:
Archaic password resets using emailed links, SMS codes and security questions remain easy targets. Even when appropriate, they're onerous and costly: Forrester says large organizations can spend $1 million annually on the infrastructure to facilitate credential resets. With liveness detection-enhanced face biometrics, your selfie can be used for any high-risk transaction, including password resets – a surefire defense against account takeovers.

Telcos:
Reports of SIM swap fraud have gone up by 400 percent in five years (source: Which? April 2020). Biometric-based identity verification and authentication solutions can help ensure that phone numbers are only transferred to the legitimate account owners. Telcos can now protect their subscribers against SIM swap fraud by leveraging biometric authentication to help call center employees separate legitimate requests from fraudulent ones.

Online dating:
Dating sites and apps can cultivate trust with users and ensure they feel comfortable putting their hearts – and their personal information – on the line. Thanks to AI and biometrics, modern dating platforms can fight catfishing, deter online fraud and help create a highly reputable community of real people.

As digital access continues to enable a remote and mobile life, new use cases will emerge, and intelligent identity technologies will be integral to maintaining trust not only in the enterprise, but also in voting, hospitality, online dating, the sharing economy, telemedicine, telcos and social media. With smart onboarding and authentication, electronic voting can anchor and maintain trust chains, encouraging citizens to exercise their rights safely and securely.

With AI-enhanced biometrics, the sharing economy can engender goodwill and trust between users, service providers, renters and hosts, creating fraud-free business environments. And as hotels reopen in the wake of the pandemic, hospitality providers can meet customers' expectations for a safe online experience, issuing mobile keys directly to smartphones, and enabling hygienic distancing practices, all while providing highly customized personal services.

Without artificial intelligence, technologies claiming identity assurance will simply not meet the demands of these ambitious requirements and use cases, which require scalable, easy-to-deploy solutions with unbreakable security and a low-friction user experience. Smart cities, smart finance, smart lifestyles – they will all be built on intelligent identity.

AI-driven biometrics and online identity verification and authentication technologies are available today from Jumio and FaceTec. To learn more, please contact:

Dean Nicolls
Vice President, Global Marketing
Jumio
dean.nicolls@jumio.com

John Wojewidka
VP of Communications
FaceTec
johnw@facetec.com

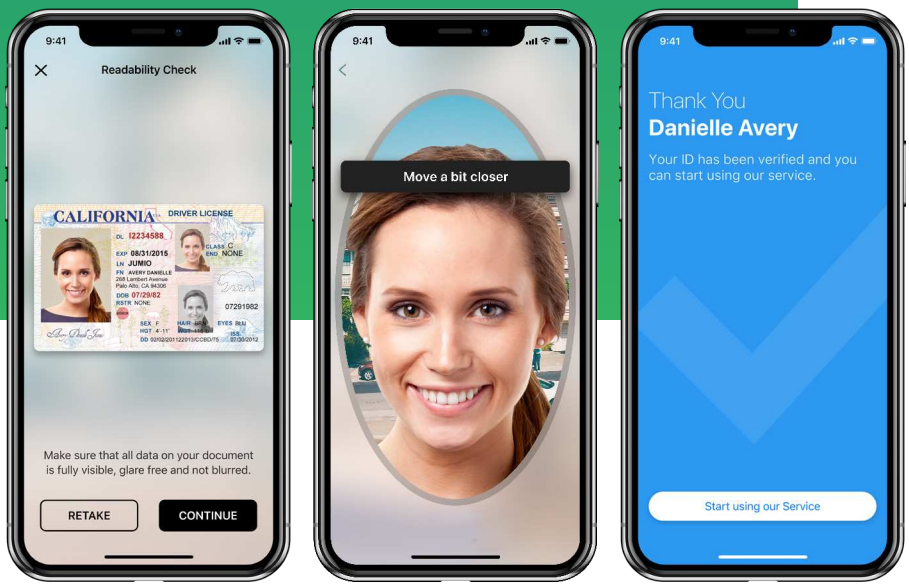
ABOUT JUMIO

When identity matters, trust Jumio. Jumio's mission is to make the internet a safer place by protecting the ecosystems of businesses through cutting-edge online identity verification and authentication services that quickly and accurately connect a person's online and real-world identities. Jumio's end-to-end identity verification solutions fight fraud, maintain compliance and onboard good customers faster.

Leveraging advanced technology including AI, biometrics, machine learning, certified 3D liveness detection and human review, Jumio helps organizations meet regulatory compliance including KYC, AML and GDPR and definitively establish the digital identity of their customers. Jumio has verified more than 250 million identities issued by over 200 countries and territories from real-time web and mobile transactions. Jumio's solutions are used by leading companies in the financial services, sharing economy, digital currency, retail, travel and online gaming sectors. Based in Palo Alto, Jumio operates globally with offices in North America, Latin America, Europe and Asia Pacific and has been the recipient of numerous awards for innovation.

For more information, please visit www.jumio.com.

jumio



ABOUT FACETEC

FaceTec's patented, industry-leading 3D Face Authentication software anchors digital identity, creating a chain of trust from user onboarding to ongoing authentication on all modern smart devices and webcams. FaceTec's 3D FaceMaps™ make trusted, remote identity verification finally possible. As the only technology backed by a persistent spoof bounty program and NIST/iBeta Certified Liveness Detection, FaceTec is the global standard for Liveness and 3D Face Matching with millions of users on six continents in financial services, border security, transportation, blockchain, e-voting, social networks, online dating and more. FaceTec was founded in 2013 with offices in San Diego, CA and Summerlin, NV.

FaceTec pioneered commercially viable Liveness Detection and is the only face authenticator to attain Level 1 & Level 2 Certifications in NIST/NVLAP-certified Presentation Attack Detection (PAD) tests, and is the world's only biometric security company with an ongoing Spoof Bounty program. FaceTec also provides an easy to use IDV Dashboard to manage the biometric authentication process, including 3D Face Matching-to-a-2D-photo-ID, document anti-tampering checks, user age estimation, duplicate checks and fraud lists, all working together to prevent identity theft and unauthorized access.

Developers can download the FaceTec demo apps directly from FaceTec.com for iOS, Android and any webcam-enabled browser, and the developer SDKs are available free at https://dev.facetec.com.

facetec