Biometric Authentication for Identity Service Providers

proov

Introduction

With losses from identity theft and fraud set to reach $721 billion worldwide in 2021, secure authentication and verification should be the cornerstone of every organization's digital strategy.

In the current digital security landscape, identity verification and authentication measures such as One-Time Passwords (OTPs), SMS passcodes, secret answers, and hardware tokens are widespread, but there are limitations to their practicality and levels of security against sophisticated digital attacks - which is why biometrics has become increasingly popular in recent years. A recent Global Industry Analysts survey predicts the biometric market to grow by 14.8% over the next 5 years.

From facial verification to fingerprint scanning, biometrics has become a staple of everyday life and the public has become increasingly comfortable using the technology. Furthermore, businesses and governments have also taken a huge step in incorporating biometric technology into their infrastructure and processes. Many organizations in financial services, e-commerce, retail, travel and the public sector have implemented biometric technology to enhance their services and future-proof their systems. Using unique biological characteristics such as a person's face, irises, fingerprints, or voice to accurately identify the user, organizations can establish and verify the identity of a person when they are trying to access an account or service. Best-of-breed biometric authentication can not only offer speed and convenience but enable verification to be done remotely with the highest levels of security.

This report explores how biometric authentication technology meets the needs of effective identity verification by delivering security, convenience, speed and a positive user experience.

Did you know?

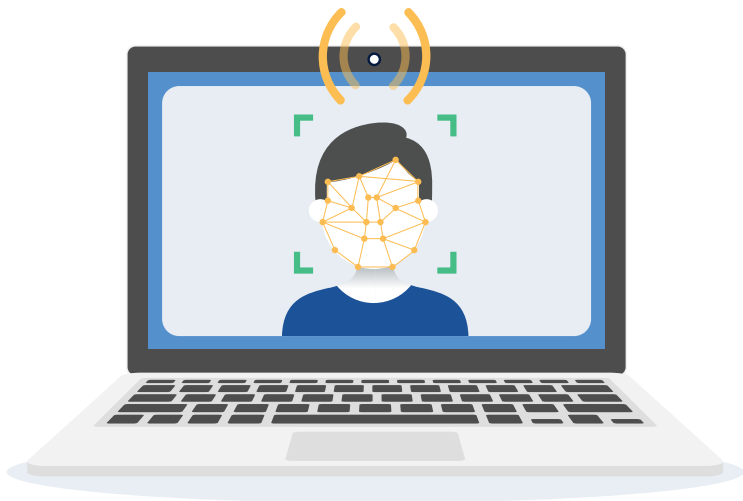
650%
growth

Worldwide, contactless payments using biometrics grew by 650% in 2020 and biometrics is projected to authenticate over **$3 trillion** of payment transactions in 2025.

Why Biometric Authentication?

Traditional security methods such as passwords are no longer fit for purpose as they leave systems and users vulnerable to hackers, fraudsters, and bad actors.

In terms of convenience, creating unique passwords for every online account is also not practical for customers and leads to bottlenecks like email resets or account lockouts. Furthermore, according to Gartner research, between 20-50% of all help desk calls are for password resets and the average cost for a single password reset is about $70!



Biometric technology can both help organizations save money and improve the customer experience. In addition, this technology incorporates secure measures for authentication and verification with a higher level of assurance than traditional methods of digital identity verification. For example, passwords are increasingly required to be more complex in an effort to improve security. However this can be counterproductive as users will typically find shortcuts to remember their password such as writing a physical note or saving it on their desktop, which leaves the organization and user at risk. Best-in-breed biometric authentication can often be a simpler and more secure solution as users only need to exhibit biological characteristics such as their face, iris, fingerprint, or voice to gain access.

Did you know?

Over **75%**

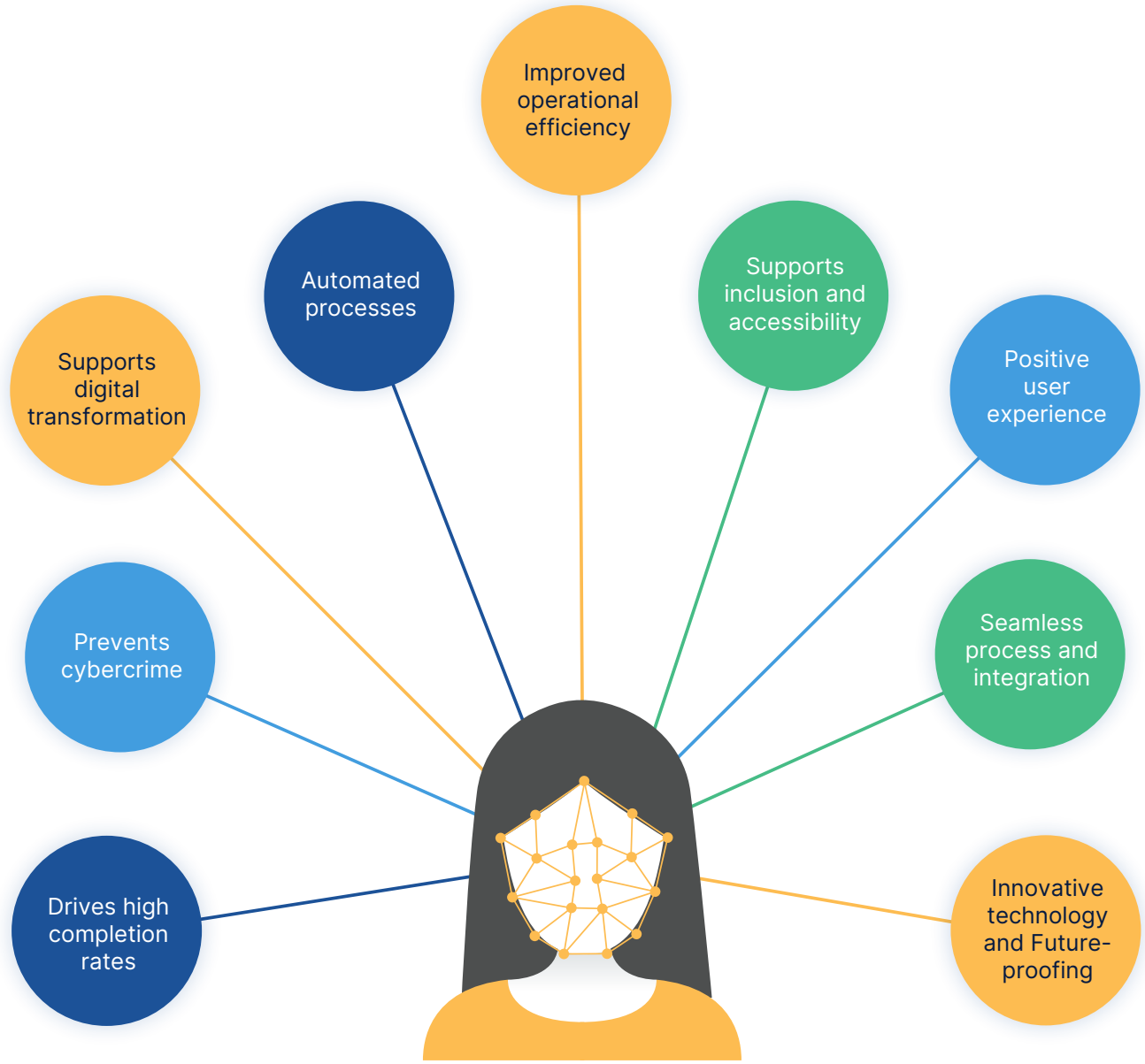
of U.S. consumers have used some sort of biometric technology? In a 2019 study regarding online payments, participants highlighted the main benefits of biometric technology were that it was quicker and more convenient than traditional verification methods such as passwords, with 44% of respondents noting each of these benefits. Another 37% also said it was more secure than other verification methods.

The Advantages of Biometric Authentication

Drives high completion rates

Today's customers are more demanding than those even a decade earlier with far more willing to take their business elsewhere if their needs are not met. With onboarding for example, it's unsurprising that the more obstacles a customer runs into, the less likely they are to complete - with around 36% of financial institutions losing a customer due to slow or inefficient onboarding procedures. Organizations must make a good first impression by delivering an effortless customer experience. Biometric authentication can streamline the onboarding process by simplifying the user experience, which leads to higher completion rates and increased revenue.

Obtaining high completion rates is a top priority for many organizations, so it's important to ensure that the balance between security and usability is adjusted appropriately to achieve this goal. Face biometric authentication solutions can deliver a secure and effortless user experience, whether it's a multi-step onboarding process or a simple authentication for a low-risk transaction. Ultimately, to achieve maximum completion rates any solution must meet security, speed, inclusivity, and convenience requirements.



Protects against cybercrime

Hackers and fraudsters are always on the lookout for gaps in security and ways to exploit organizations and their users. Traditional authentication processes such as passwords are easy targets for attackers. Passwords are frequently lost, forgotten, manipulated, or stolen meaning they are not accurate in confirming a user's authenticity as criminals can repurpose credentials. Without secure verification, a fraudster can use fake or stolen identities to access services. Wider data breaches that expose usernames and passwords also weaken the integrity of the security process, exposing businesses to risk and impacting their reputation with customers.

As criminal methods become more advanced, organizations must find new ways to defend against these attacks. Biometric authentication can robustly reinforce fraud prevention efforts and help ensure the right user is accessing their accounts. For example, when verification is required to onboard a customer, a selfie-style biometric face scan can be completed quickly and effortlessly on the user's personal device. This presented image is then matched to a verified document and checked for liveness. This process protects against cybercrime during remote enrollment and authentication by accurately verifying that the remote individual is the right person and a real person. Genuine Presence Assurance also provides the critical additional check that the individual is interacting right now. This delivers thorough and sustainable security measures that defend against sophisticated attacks, working to provide considerable protection while also delivering an effortless user experience. Biometric authentication that is supported by cloud-based services offers a rigorous defence that is flexible and adaptable in combating evolving threats, as opposed to device-based authentication that features static defences that can quickly become outdated and vulnerable.

Did you know?

450%

increase

in attacks involving usernames and passwords translating into more than **1.48 billion** compromised records in the U.S alone, according to a 2021 ForgeRock consumer identity report.

Automated processes and increased efficiency

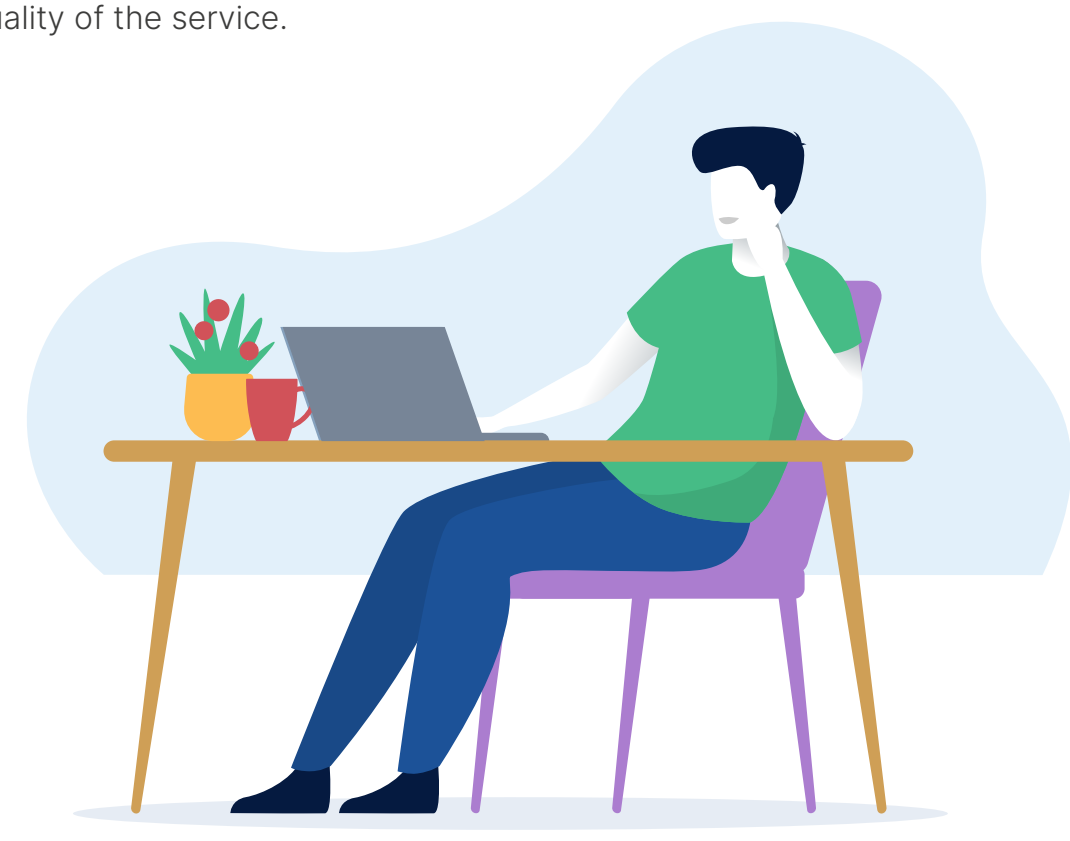
Manual verification and authentication processes, whether in-branch or via a call center, can impact the quality of the service that you deliver to your customers. These traditional, in-person methods of validating new clients are inconvenient and costly for both the organization and the customer. Manual verification and authentication processes increase costs and cannot be easily scaled - a sudden increase in new customers will require an increased manual effort, which can impact the quality of the service.

Biometrics can replace manual verification to both reduce overall costs and increase accuracy. iProov's Genuine Presence Assurance is device agnostic and offers seamless integration with current platforms. The technology is quick, secure, scalable, and more reliable than humans when it comes to verifying identity. It also bolsters fraud prevention efforts and speeds up the onboarding process, which works to maximize customer completion rates and reduce drop-off during application.

Did you know?

90% reduction

in customer onboarding costs with digital ID-enabled processes according to a McKinsey report.



Supports digital transformation

In recent years, enterprises in the private sector have reacted swiftly to become a part of the burgeoning digital economy. Seeking to meet the evolving needs of modern consumers, these businesses have enhanced their infrastructure and operations to provide digital solutions.

While the impact of COVID-19 has accelerated the rollout of digital programs, legacy manual processes have impacted many organizations' ability to meet customer expectations of an effortless user experience. However, incorporating biometric authentication can enable secure and efficient access for customers, increase operational efficiency, and reduce fraud. This technology can also future-proof infrastructure, enabling businesses to safeguard their customers in an ever-turbulent threat landscape while also providing convenience.

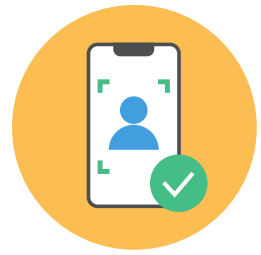
Inclusive and accessible

For a digital solution to be widely adopted it must be inclusive, and services provided online must be simple to use, regardless of age and education, and offer convenience rather than obstacles for a customer. The ubiquity of mobile and tablet device usage across multiple demographic groups provides a universal platform and incorporating best-of-breed biometric solutions can increase inclusivity and accessibility for onboarding and ongoing verification. Traditional methods like visiting a branch may be difficult or impractical to access for some people, so providing a secure online alternative that supports customers in multiple regions and diverse populations is necessary. However, for those that do not possess a smartphone, or require additional assistance in person, biometric self-serve kiosks also represent a secure physical option.

Biometric authentication can provide a secure online option that ensures the right person is accessing this service, delivering inclusive access irrespective of age, literacy, language, cognitive ability, disability or other constraints. Furthermore, this technology also delivers increased operational efficiency as human resources can be reallocated to areas where they are most needed, rather than on administrative tasks.

Provide a positive user experience

While the chief role of any identity verification solution is to provide security, delivering a positive user experience is almost as important. A recent Ping Identity survey stated that 63% of consumers are likely to leave an online service for a competitor who makes it significantly easier to authenticate their identity. If multi-factor authentication (MFA) is not implemented correctly, it can add layers of verification for users to prove their identity, which typically results in a frustrating user experience and may also be counterproductive in producing higher security and preventing fraud.



47%

of users said mobile biometric verifications by a financial institution's call center would improve the experience (OWI).

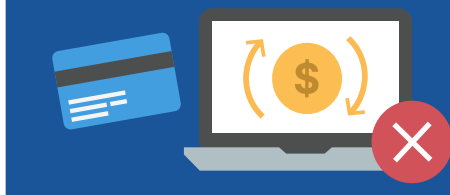
73%

of organizations from various sectors are using biometrics to ensure good customer and user experience (Goode Intelligence).

56%

of online consumers have abandoned an online service when logging in was too frustrating. Additionally, **63%** of consumers are likely to leave an online service for a competitor who makes it significantly easier to authenticate identity (Ping Identity Survey).

Did you know?



66%

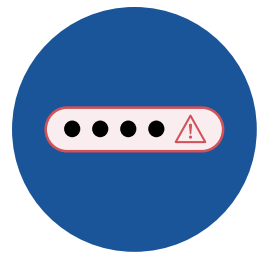
of customers

abandoned account openings or transactions due to long signup or payment process. OWI Whitepaper.

Today's customers expect to be able to complete even the most secure processes online without going into a branch, contacting a call center, or dealing with lengthy verification procedures. These users expect processes to be simple and fast. Nonetheless, modern organizations must ensure that the correct and necessary checks are completed with high degrees of accuracy as well as meeting the needs of the customer. Biometric technology, such as facial verification can combat this issue by providing a solution that allows institutions to conduct the rigorous checks they need to comply with compliance regulations while also providing a straightforward, seamless experience for the user. Banks such as Knab and Rabobank have embraced this onboarding strategy and are embracing effortless, automated customer experiences that minimize drop off and deliver high customer satisfaction.

40%

are not able to answer their security questions at least half the time when trying to regain access to an account or resetting a password (*Ping Identity Survey*).



61%

of US consumers have stopped using an account or online service because they became frustrated when trying to sign in (*Ping Identity Survey*).

Conclusion

The business world is continuing its unrelenting march towards a digital future, so possessing a secure and accessible digital identity is a necessity. Current security measures, such as passwords, PINs, OTPs and other MFA methods are causing friction with users and are incapable of meeting with the security needs of modern identity verification providers.

Biometric technology however offers a way of not only meeting existing user requirements but future-proofing infrastructure against potential threats that may come down the line. As fraudsters become more prevalent and brazen, the need for secure biometric authentication will only increase. Machine learning and artificial intelligence can help assess and combat digital attacks in real-time, reducing the risk of reputational damage, lost business, and impact on customers.

Identity verification providers looking for a solution that provides flexibility, ease of access, and high assurance should focus their sights on biometric authentication.

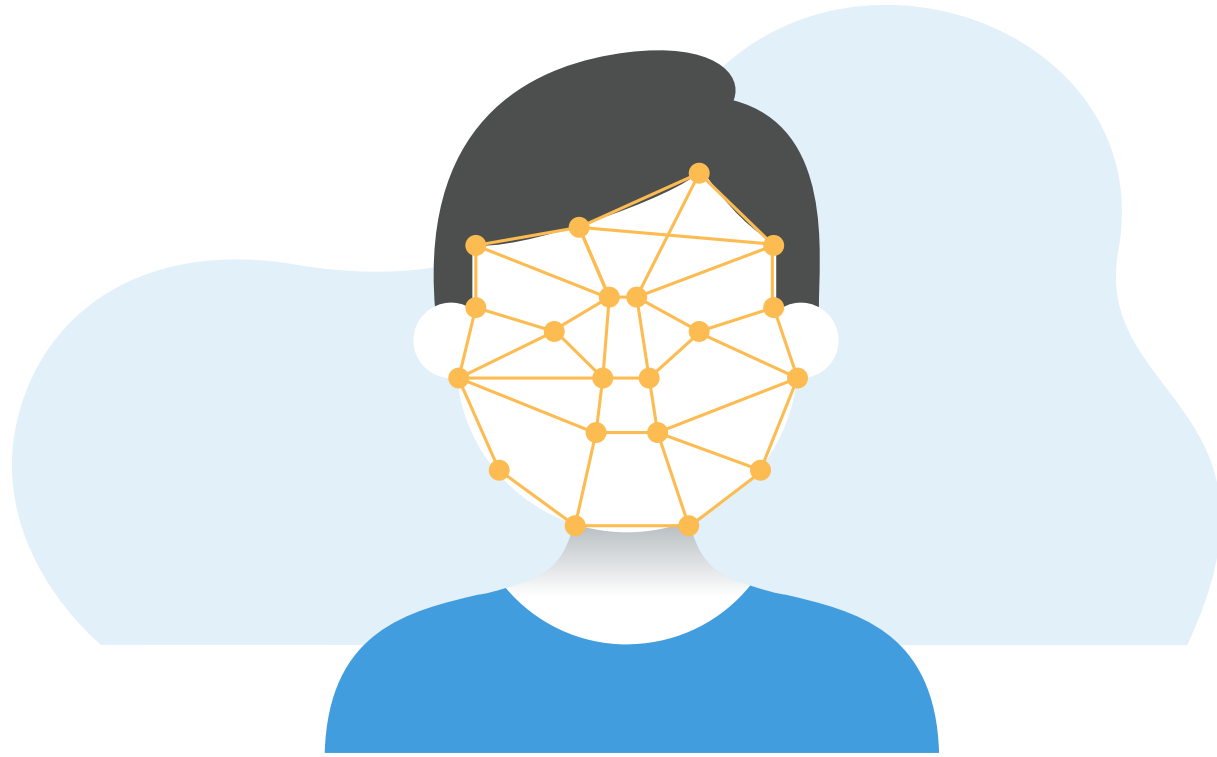
Biometric technology can help to:

- Bolster system and user security
- Improve the user experience
- Increase speed and convenience
- Reduce costs and increase time-savings
- Future-proof infrastructure

Interested in learning more about how biometric authentication can support your digital transformation? Visit iProov.com.

iProov provides facial biometric technology to governments, financial institutions, and other enterprises that need to securely authenticate customer identity online. iProov has partnered with many identity verification providers including Jumio, Innovalor, iiDENTIFii, and WorldReach (an Entrust Company) and is a trusted provider of face biometric verification and authentication solutions that are fully optimised for usability, accessibility, security, and privacy.

Follow us on LinkedIn and Twitter for the latest news and industry updates.



For more information on how to assure the genuine presence of the **right** person, **real** person, authenticating **right now** contact us at:

contact@iproov.com

iproov.com