Biometric Authentication for Financial Services

Introduction

Today, the need to physically visit a bank or other service provider continues to dwindle as many processes shift to digital. The need for secure online identity verification is more important than ever before. From banks to governments, many organizations require a user to verify their identity before they can access services with levels of security varying based on operational and transactional risk.

Many organizations in the financial sector such as retail banks, investment banks, wealth management firms, payment providers, and cryptocurrency exchanges have to strike a balance between executing swift and accurate verification of new customers while delivering a positive user experience. No simple feat, but with every challenge comes opportunity.

Let's take a closer look at biometric authentication.

What is Biometric Authentication?

Authentication is the process of establishing someone or something as genuine, true, or valid. The biometric element refers to using unique biological characteristics such as a person's face, irises, fingerprints, or voice to accurately identify the user. In the digital sphere, authentication means establishing and verifying the identity of a person when that person is in the act of claiming or asserting that identity.

Biometric authentication enables this to be done remotely with the highest levels of security. During an online onboarding process, for example, customers can be asked to use a mobile device or computer to scan a trusted identity document such as a passport or driver's license to verify their identity. In this instance, they would then complete a biometric face scan to confirm that they are who they claim to be. Once the customer has onboarded, ongoing biometric authentication can confirm a user's unique biometric characteristic against the template created during this initial verification process.

There are certain key processes where biometric authentication is typically implemented for financial services organizations:

Onboarding

To protect against new account fraud and comply with KYC and BSA/AML regulations, financial institutions can use biometric authentication for remote onboarding. A new customer can complete the identity verification stage on their mobile device or computer to verify that they are who they claim to be.

Ongoing Authentication

Once the user has onboarded, they need an appropriate level of security for future authentications. Biometric authentication can be used for actions of all risk profiles, from sensitive transactions such as requesting a new debit card or changing a PIN to checking a bank balance.

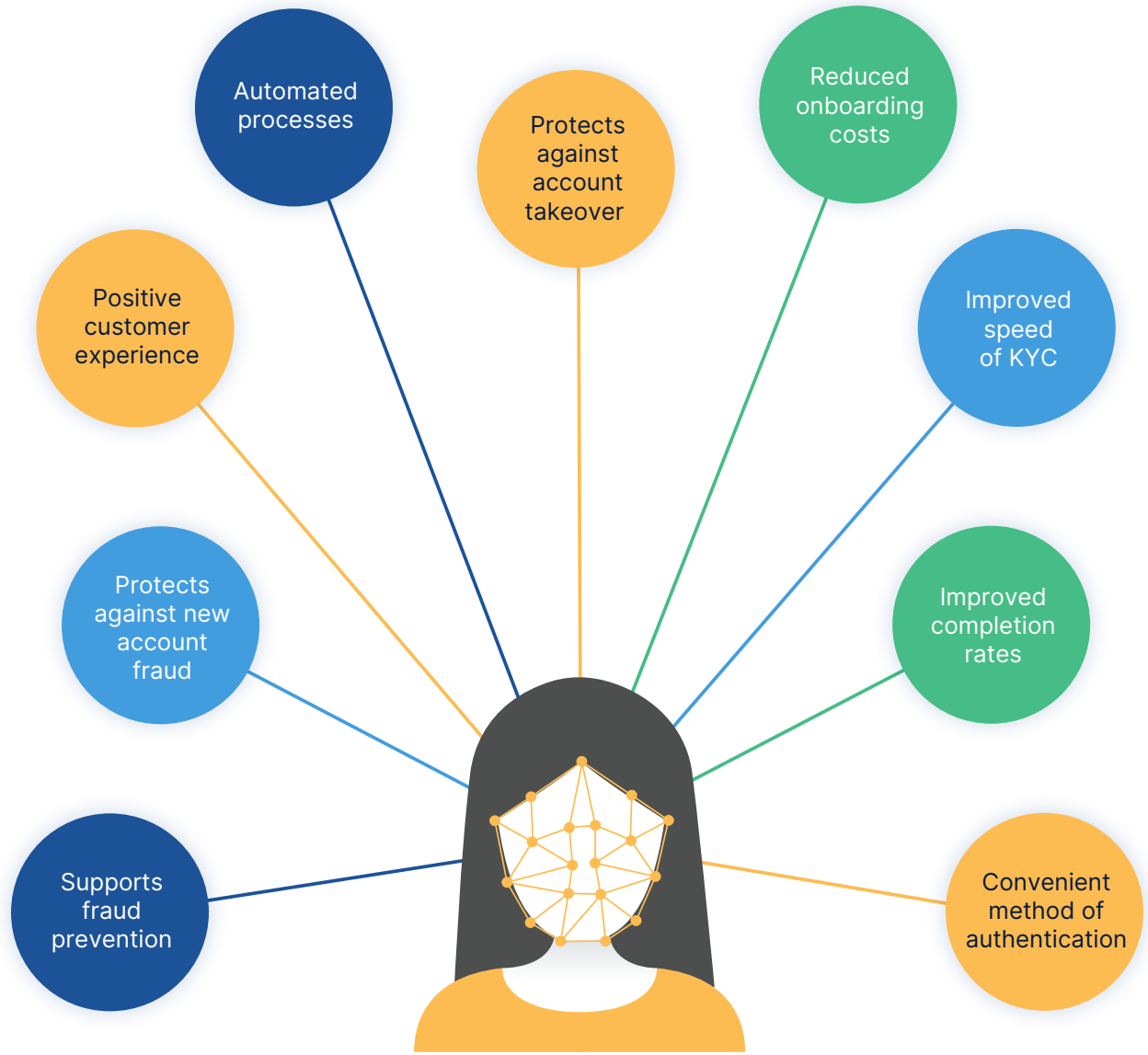
Identity Recovery

What happens when a customer upgrades or loses their mobile device, or it's stolen or broken? It's important to enable the genuine user to effortlessly recover their identity while keeping the imposters out. In particular, cloud-based biometrics are able to provide the strong authentication needed to recover the identity of the owner of the device.

The Advantages of Biometric Authentication for Financial Services

Drives high onboarding completion rates

Today's customers are more demanding than ever, and are more willing to take their business elsewhere if their needs are not met. It's unsurprising that the more obstacles a customer runs into, the less likely they are to complete the onboarding process - around 36% of financial institutions say they have lost a customer due to slow or inefficient onboarding procedures, so 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.



Helps to prevent 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, present an easier target. Passwords can be shared, guessed or stolen, which means they are not reliable in confirming a user's authenticity, as criminals can repurpose credentials. Also, data breaches that expose usernames and passwords weaken the integrity of the security process and expose the individual or organization to risk. Without secure verification, a fraudster can use synthetic identities to open bank accounts (**New Account Fraud, or NAF**) and criminals can also gain access to legitimate bank accounts (**account takeover**).

As criminal methods become more advanced, financial institutions must find new ways to defend against these attacks. Biometric authentication can robustly reinforce fraud prevention efforts and help organizations ensure the right user is accessing their accounts. For example, when verification is required to onboard a new customer, a biometric face scan can be completed quickly and effortlessly on the customer's personal device. This provides protection against cybercrime by accurately verifying a customer's identity at onboarding and then ensuring the secure ongoing authentication of users to prevent any future account takeover. Technology like Genuine Presence Assurance delivers a thorough and sustainable security measure that defends against sophisticated attacks. This provides the organization with considerable protection while also delivering a straightforward user experience.

Did you know?

80%

of hacking-related breaches involve compromised and weak password credentials

(Verizon's Data Breach Investigations Report)

Automated processes and reduced onboarding costs

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 for the customer and costly for the financial institution. A McKinsey report highlighted that digital ID-enabled processes can provide a potential 90% reduction in customer onboarding costs. Manual processes are also difficult to scale - a sudden increase in new customers will require increased manual effort, which is costly and difficult to deliver quickly.

Biometric authentication can replace or enhance manual verification to both reduce overall costs and increase accuracy. 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.

Provide a positive customer experience

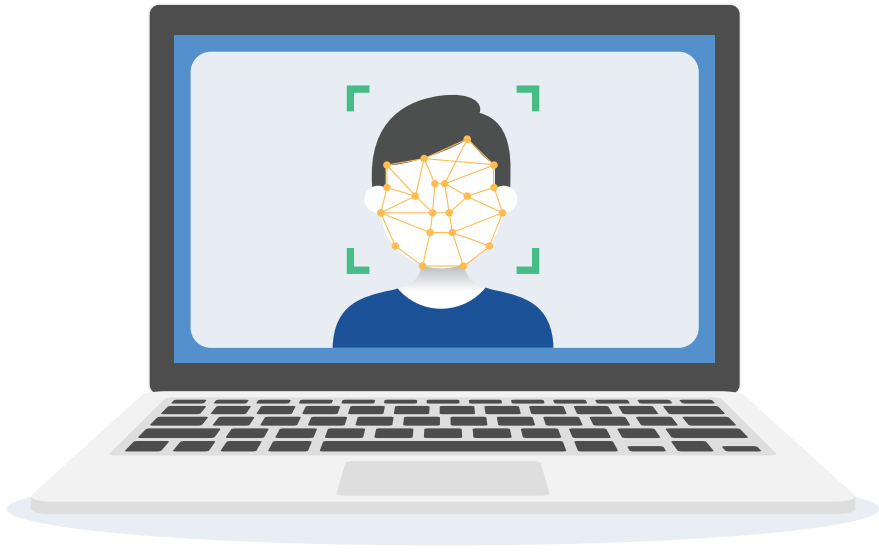
Most bank customers expect to be able to complete even the most secure processes online without going into a branch or contacting a call center. These users expect processes to be simple and fast. Financial institutions must ensure that the correct and necessary checks are completed with high degrees of accuracy as well as meeting the needs of the customer.

Biometric authentication such as facial verification allows institutions to conduct the rigorous checks they need to comply with BSA/AML and KYC regulations while also providing a straightforward, seamless experience for the user. Challenger banks have embraced this onboarding strategy and are setting a precedent for effortless, automated customer experiences that minimize drop off and deliver high customer satisfaction.

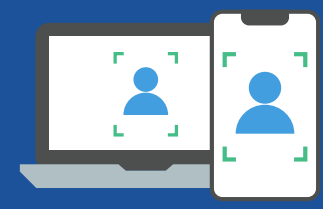
Everyone's already using it!

Did you know that over 75% of U.S. consumers have used some sort of biometric technology? In a 2019 study on online payments, participants highlighted that biometric technology offered benefits of speed and convenience over traditional authentication methods. In addition, around 46% of Americans are currently using digital financial services, highlighting the importance of convenience and customer experience when choosing a service provider.

Over the past decade, biometric technology has become a staple of everyday life. Ranging from facial verification to fingerprint scanning, the public has become increasingly competent, comfortable, and experienced in the use of biometric technology. Face authentication, in particular, has a major advantage over other biometric options as it does not require specialist hardware; most devices have a front-facing camera, making facial authentication available to a large portion of the population.



Did you know?



70%

of Americans that use mobile banking either already use face authentication to access their banking app or would do so if it was supported.

Source: iProov survey

Why do Financial Institutions Need Biometric Authentication?

Win at Digital Transformation

Whether it's attracting new digitally native customers, saving money or streamlining processes, digital transformation goals can be achieved with biometrics.

Meet Demand for Digital Simplicity

Customers increasingly expect a simple, hassle-free digital experience. Biometric authentication replaces the hassle of passwords or security questions.

Compete with Challengers

Digital banks are able to offer a fantastic online customer experience. It's important for other institutions to offer digital services that can compete.

Maintain Customer Trust

Consumers are increasingly concerned about data privacy and identity theft. Financial institutions need to maintain customer trust with secure authentication.

Prevent New Account Fraud

Financial institutions must be able to securely verify the identity of a remote customer during onboarding. In 2020, identity fraud accounted for losses of $56B in the financial sector.

Prevent Account Takeover

Biometrics can strengthen online account security to protect against account takeover and potential fraudulent activity from unauthorized account access.

Prevent Money-Laundering

In the fight against organized crime, biometrics can enhance security efforts and help protect against fraudulent activity.

Comply with Regulations

Stringent KYC and BSA/AML regulations demand that organizations execute due diligence with every new customer. Avoiding penalties and negative press coverage relies on secure online identity verification and authentication.

Interested in learning more about how biometric authentication can improve your business?
Visit iProov.com.

iProov is the world leader in providing facial biometric authentication technology to financial institutions, governments and other enterprises that need to securely verify customer identity online. Used for onboarding and authentication, iProov customers include Rabobank, ING, the US Department of Homeland Security, the UK Home Office, Singapore GovTech, the Australian Taxation Office and others.

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