BIZCOMMUNITY

Biometric authentication is no longer a business enabler - it's now crucial for long-term success

By Gur Geva

7 Sep 2022

Remote digital biometric authentication and verification are now firmly in the mainstream thanks to the need for businesses to be continuously active online.

Source: Supplied. Gur Geva, the co-founder and chief executive officer of iiDENTIFii,

For this reason, technologies involving proven facial biometrics to onboard or authenticate customers, employees, suppliers, or the like, have become critical for the security of business operations, and for security and fraud-prevention reasons.

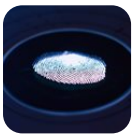
Using biometrics to access services has largely been popularised through mobile phones and increasingly the need for secure, complicated passwords is being replaced by biometrics. With the pervasiveness of mobile ever-growing, technology adoption is no longer only for the digital elite.

As a result, organisations are now trending towards digital biometric authentication instead of passwords for ease of access, and the type of biometric authentication is evolving, too. In fact, biometric authentication is more than an enabler; it

is critical for the sustainability and longevity of any successful business.

Not only are businesses compelling their clients to onboard digitally using remote facial biometrics – as one of the most accurate and reliable form of biometrics – but customers also feel more comfortable using facial biometrics to transact digitally with organisations instead of uploading personal details.

The uptake of remote digital biometric authentication is no longer inconvenient, or an obstacle, for customers. On the contrary, it gives them reassurance.



Icasa linking SIM cards to biometrics - how new regulations aim to keep consumers safe

10 May 2022

As the zero trust security model gains traction, customers demand that the companies that they are dealing with in the online digital world are real, trustworthy, and secure. Today's customers want the necessary assurance that they can transact without the fear of being defrauded or becoming a victim of identity theft.

More people onboarding

A study published in *IEEE Transactions on Technology and Society*, reveals that most people are comfortable with biometrics given the right circumstances.

Furthermore, biometric methods promise better user experience and trust and accountability benefits than other credential-based methods and are fast gaining traction as a result with end-users across various markets.

Device-native biometric methods are now standard in new phones, tablets and PCs and are readily integrated into mobile apps, browser-based apps, and proprietary authenticator apps for smartphones. In addition, third-party biometric methods offer greater control over enrolment and configuration, better omnichannel support, and integration with identity proofing.

Customers are no longer inconvenienced by having to biometrically onboard but rather feel reassured that the respective company has the correct security in place to protect their transaction and their identity.

People transact on several hardware devices or operating systems, laptops, phones, Android, and iOS, so where there are people and devices, there is a need for trust to be able to transact.

Risk and governance

Biometric authentication is not only important for security but also from a risk and governance point of view, especially as

regulations attempt to keep pace with online digital growth.

Governments around the globe are enacting laws around remote trade and communications where personally identifiable information is protected, and companies need to prove they have taken reasonable steps to protect consumers and their information from theft and fraud.

Biometric facial-recognition technology takes off at German airports

29 Apr 2022

Establishing a relationship of trust is also not only for the customer but for the organisation themselves too – and biometric authentication is a critical tool to establish that trust.

Prioritising first point of entry

For a true and trusted engagement to be cemented, organisations require three things of you:

- Something you are (biometric);
- Something you know (for example a password or ID number), and
- Something you have (hardware device).

Advanced biometric authentication is the first point of entry into an organisation's digital world and should be a priority and non-negotiable within a security and risk strategy.

As people have become comfortable with taking selfies, the familiarity of holding a phone up to their face has added to the exponential growth of facial biometric authentication, which very soon, will become as normal and mainstream as PIN codes are now.

ABOUT THE AUTHOR

Gur Geva is the co-founder and chief executive officer of iiDENTIFii, provider of remote biometric digital facial authentication and automated onboarding technology.