Why biometric technology is key to digital transformation for SA banks

By Lance Fanaroff

5 Sep 2019

As South Africa's banking sector embarks upon digital transformation and the shift to branchless banking, cybersecurity and fraud prevention will have to be top of mind.

Lance Fanaroff, director at iiDENTIFii

Indeed, while the race to provide quick and efficient mobile banking solutions is driving innovation, it also creates new opportunities for shrewd cyber criminals and hackers. As it stands, the South African Banking Risk Information Centre (SABRIC) reported that in 2018 digital banking fraud across all platforms resulted in over R262 million in losses, with the number of incidents increasing over 75%.

In the face of this challenge, many banks are being forced to rethink their security procedures – while also balancing increasing consumer demand for a mobile and friction-free banking experience.

Today, the growing pressure to strike this balance has been driving increasing adoption of biometric technology solutions amongst banks and other financial institutions. Put simply, biometrics refers to the use of technology to identify a person based on some aspect of their biology.

While the use of biometrics used to be limited to governments and high security environments, rapid advancements in the technology – coupled with increasing smartphone penetration – are making biometric solutions ever more attractive (and accessible) for banks looking to digitise their processes.

The benefits of using tech to create government ID's

Joby Mathew 29 Jul 2019

Indeed, by harnessing the sophisticated cameras, sensors and rich applications that smartphones now offer, banks can explore new solutions that meet customer demands for mobile, quick and engaging banking capabilities.

One such example is remote on-boarding: by using advanced biometric digital authentication technology platforms, savvy banks can now enable new customers to open accounts and begin transacting without having to go into a branch and submit reams of paperwork. This type of capability will arguably become more and more important as banks compete to win market share amongst demanding, digitally savvy young customers.

‘Liveness’ detection is key

While interest and investment in biometric authentication technology is rising in line with rapid digitisation, it is imperative that banks choose robust solutions. When harnessing biometric technology to prevent fraud, the key element is liveness detection: the ability to determine whether the source of a biometric sample is a live human being or a fake representation.

Today, many banks and organisations are using gesture-based biometric techniques. This is problematic and represents a security vulnerability because this technology is quite easily spoofed and/or hacked.

The yesterday, today and tomorrow of biometrics

Christian Fredrikson 6 Jun 2019

With this in mind, it is critical that banks explore newer and more advanced biometric authentication solutions that have more sophisticated liveness detection capabilities. For example, there are new solutions that leverage facial algorithms and 3-D image detection – thereby achieving accurate proof of liveness with a facial recognition system that is multiple times harder to spoof.

Balancing innovation with efficient processes

In addition to choosing a biometric authentication solution that is current and leading edge, banks and organisations have to ensure that implementation is managed correctly. This is key to ensuring that the solution is safe and robust, as well as enabling a smooth end user experience. When harnessing biometric on-boarding solutions in particular, it is critical that the customer experience is as seamless and friction-less as possible – thereby supporting the broader move to efficient, digitised, branchless banking.

Internally, banks should place strong emphasis on the process flow – which requires having skilled managers in place to guide the integration of new biometric solutions within existing infrastructure. Similarly, banks have to choose their technology partners very carefully, and drive a transparent, highly engaged partnership to ensure that biometrics are integrated in the most agile and efficient way.

There is inevitably a great deal of governance, administration and red tape involved in any rollout – so it is imperative that every key stakeholder is engaged and supportive of the integration process.

Notably, the right technology partner should also advise on the most recent advancements and trends within biometric authentication and fraud prevention that are impacting the global financial services sphere. For example, as customer databases become more important and serve as competitive differentiators, banks should explore blockchain technology as a way of securing highly sensitive biometric data.

Looking ahead, biometric databases will need to be impenetrable – and blockchain technology can arguably fulfil this requirement while also supporting ongoing innovation within banking.

Embracing a future-proof security solution

There is no doubt that the digital race is on: banks are now competing to win the loyalty of increasingly fickle, demanding and digitally native customers. The winners will almost certainly be the banking providers who can effectively balance the need for mobility and convenience with robust security and sophisticated fraud prevention.

Today, biometric authentication technology is proving to be one of the most reliable ways of achieving this balance, and will potentially become even more integral to banking security in the years to come.

ABOUT THE AUTHOR

Lance Fanaroff, director at iiDENTIFii