Bypassing The Password

By Somna Trehan

Biometrics Will Widen The Scope of Mobile Banking

Biometrics are serving a critical role in mobile banking today. In a recent survey; 79% of respondents mentioned that they prefer biometric authentications and believe that mobile apps with biometrics are more secure. In fact, 42% said they would not use a banking or payment app if it doesn't offer biometric authentication[1].

Keep in mind, every extra step of authentication causes friction and frustration for your customer and may ultimately result in consumers abandoning your mobile banking app. Biometrics are becoming popular because they help in reducing this friction in transactions; and despite the ease of use, they are more secure than the password based authentication process.

Banks need to find a balance, because while simplification reduces friction and improves convenience for some, others may perceive it as a weak security policy. Banks need to assess the convenience and sensitivity of consumers regarding the usage of biometrics and find a procedure that is best suited for their expectations.

So what are the various biometric technologies available that banks can leverage now? The technologies range from iris to voice authentication. Some like fingerprint recognition have been in use for over a decade and are more mature, while others like face and vein recognition are more recent. The choice depends on the following factors:

Security: Does the technology ensure security and consistency of output? Will it be spoof-resistant and provide confidence to the consumer for transacting over mobile?

Convenience: Does the technology improve customer convenience as compared to the current authentication process? Does it drive higher mobile banking transactions and inspire more customers to opt for mobile banking?

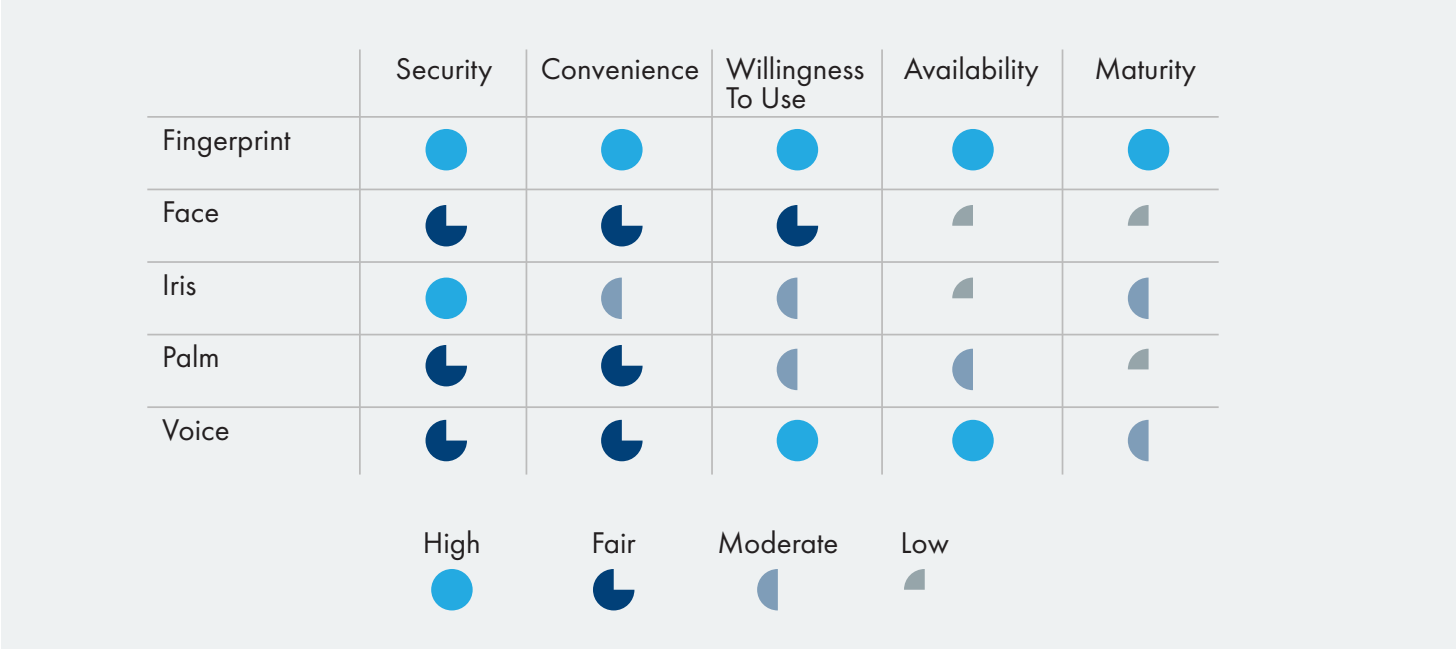
Willingness to use: Are the customers comfortable in following the authentication process? For example, some may not be comfortable in speaking out a sentence or clicking a picture of their palm in a crowded place.

[1] Source: The Retail Banking Biometrics Confidence Report (2017); Eyeverify

Availability: Which technology is most readily available on mobile devices of banks' customers to ensure sufficient uptake of the new authentication process?Digitizing the onboarding experience can also drive significant cost savings.

Maturity: Is the technology mature enough to be used for day to day transactions? The technology should have been tried and tested and consumers should be aware of and educated on its usage before it is applied to banking transactions.

The following chart offers a comparison of various biometric technologies:



Fingerprint Scanning

Fingerprint scanning is a mature, tried and tested technology that has been in use for many decades. Mostly used by government organizations for biometric databases, it is also becoming more readily available in smart phones for user identification. It's quite convenient to use and has minimal resistance from consumers to scan fingerprints.

Facial Recognition

Facial recognition is a relatively new technology and has been introduced in smart phones only recently by Apple with its recently released iPhone X. It should soon become available on other phones as well, because competitors want to catch-up with Apple.

Face recognition technology still needs to evolve and currently may not be the most reliable biometric technology, as there could be matching errors due to difference in light, accessories, or facial hair, for example. Also, it may not be very convenient for consumers to click a selfie at a crowded/public place for facial recognition.

Iris Recognition

A person's iris is the ideal part of the human body for biometric identification because it is an internal organ protected by the cornea, yet externally visible. Iris recognition is highly reliable in terms of accuracy; as there is virtually zero probability of two people having the same identification features. However, many commercial iris scanners can be tricked by a high-quality image of an iris or face in place of the real thing.

Although it is convenient to use, some consumers may be concerned about its impact on their eyes and vision due to the scanning technology. It is a relatively new technology as compared to fingerprint recognition, and it's still not a common feature available on all smart phones.

Voice Recognition

Voice recognition maps several aspects of a consumers' voice such as pitch, accent, pronunciation, breathing, etc. with existing records. Like fingerprint recognition, voice recognition is relatively more user-friendly and popular compared to other biometrics. Limitations include matching errors due to quality of audio samples being affected by ambient noise levels, changes in behavioral attributes, and differences in voice caused by different phones used. It's vulnerable to be misused as voice samples of the consumer can be collected from different sources and aggregated to trick the system.

Palm Recognition

Similar to face recognition, palm recognition is also relatively new and involves taking a picture of the user's palm and comparing it with the image in a database for identification. Since palms are unique and do not change with age, they can be used for secure biometric authentication, although high resolution pictures may confuse the system with a real palm. Other pitfalls include matching errors due to hand pose variations, complicated backgrounds, and different light conditions.

All the technologies discussed above have their benefits and downsides. Many are new, and will evolve and become more secure and user-friendly sooner rather than later. However, one thing is for sure: we will be using fewer passwords in the future.

Banks may choose security technology based on their typical consumer's profile and preferences or go for multi-modal biometrics, which is verifying multiple biometrics to authenticate someone. As banks adopt biometrics for consumer identification, they will need to be particularly diligent on the following aspects:

Technology Provider/Partner: The technology provider they engage with should be able to provide both high-end biometrics and integration with their mobile app as well as the banks' existing systems

Scalability and Choices: Scalability and customization for different customers, regions, and features is a must. There should also be a choice of deploying biometric technology and its usage based on customer preferences.

Speed of Deployment and Reliability: While speed of deployment and reliability are crucial, banks need to be aware of how they can/will impact their investment in biometric technology. Will the results be up to par?

Biometric technology holds promise, and when utilized correctly by banks, can help create frictionless—and more importantly secure—financial transactions via mobile apps.

Want to #GrowWithTemenos? Contact us today.

Temenos AG (SIX: TEMN) is the world's leader in banking software. Over 3,000 banks across the globe, including 41 of the top 50 banks, rely on Temenos to process both the daily transactions and client interactions of more than 500 million banking customers. Temenos offers cloud-native, cloud-agnostic and AI-driven front office, core banking, payments and fund administration software enabling banks to deliver frictionless, omnichannel customer experiences and gain operational excellence.

Temenos software is proven to enable its top-performing clients to achieve cost-income ratios of 26.8% half the industry average and returns on equity of 29%, three times the industry average. These clients also invest 51% of their IT budget on growth and innovation versus maintenance, which is double the industry average, proving the banks' IT investment is adding tangible value to their business.

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