wipro.com

Mobile Biometrics: The game changer in banking

From selfies to voice recognition, smart phones are redefining the contours of mobile banking, making transactions faster and more secure

Joe's smartphone reminded him he needed to do a quick money transfer to his brother's account for tuition fees. With a simple swipe and fingerprint authentication, he opens up his mobile banking app. Since the amount is big, Joe is further prompted to do a facial biometric authentication. He looks into the phone camera and blinks, and pronto the transaction gets confirmed!

Passwords and PINs are passé; mobile biometrics is taking the banking industry by storm.

The smartphone has altered the market for biometrics in mobile banking. The days of kiosk-based, password-enabled transactions will soon be a thing of the past. The in-built smartphone cameras, fingerprint sensors, microphones now let users employ their own hardware to capture their facial, fingerprint and voice characteristics, paving the way for what we call "multi-factor" biometrics.

Mobile biometrics has caught the imagination of the digitally-empowered banking consumer. From reduced incidents of fraud and faster transactions to higher accuracy and authentication (refer figure 1); mobile biometrics has brought in a new dimension to banking on the go.

Today's smart phones can even secure and locally store (encrypted) the biometric templates instead of the centralized servers doing that.
And that is clearly a game changer.

Figure 1: Go as you like

Chink in the armor

While smartphones with sensors have made biometric technology more accessible and mainstream, giving passwords a run for their money, the transition does come with its share of challenges. One such challenge is the security risk associated with data leakages.

The uniqueness and the immutable nature of biometric data, which is its USP, can also turn out to be its biggest Achilles' heel. A stolen password can always be changed by the user whereas a user's biometric data is permanently compromised. There have been many instances where the fingerprint (widely accepted biometric option) data has been either replicated or stolen by hackers.

"The 'non-perishable' nature of certain biometrics is driving serious concern in security circles," says CEB Executive Advisor, Jason Malo, "While biometrics are easier to use than passwords, when they are compromised they cannot satisfy the security role for which they were implemented."

The Iris recognition technology is, thus, becoming more widely accepted and may soon replace fingerprints since it is not only cheaper to implement but also difficult to replicate, and, thereby, more secure.

The other challenge relates to the overall customer experience and makes it as seamless as possible across all mobile devices. For instance, not too many smartphones offer fingerprint sensors. If banks can offer both fingerprint and the facial recognition options, customers can use a wider range of devices. In fact, smartphones with as little as a 1 mega-pixel front-facing camera can offer the facial recognition option and this covers probably the entire smartphone market.

Yet another challenge is the need for standardization of biometric data when multiple vendors are involved in the process. Often, banks need to decide whether to offer uni-factor biometric options or go for multi-factor authentication (refer figure 2).

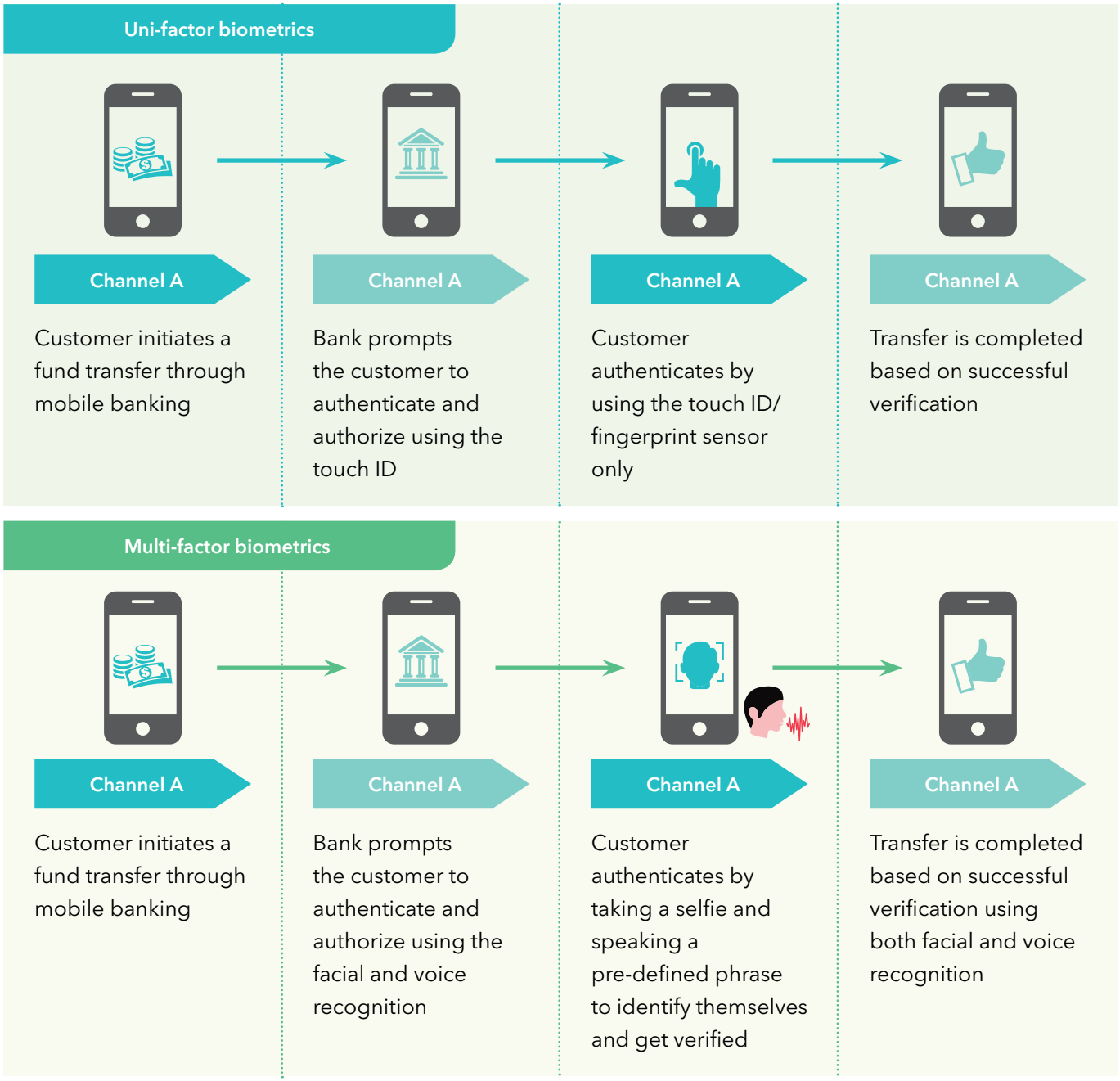

Figure 2: From single to multi

While they roll-out biometric options for clients, banks need to weigh parameters including accuracy (FAR/FRR), speed, social acceptance, verification vs identification, barriers to attack and ease of deployment. For instance, a private bank that has very high security threshold for their high net-worth clients may opt for Iris instead of fingerprint or voice, even though Iris may score low on ease of deployment or social acceptance.

Often, we do not see banks restricting to just one biometric option for their clients. Based on the transaction risk, they may opt to mix and match the options by requiring only the fingerprint to login but asking for a combination of Iris and voice to initiate a large dollar transaction (multi-factor).

An inflection point

Biometrics in banking is at an inflection point with improvements in technology on an almost daily basis, making it an extremely compelling option for both banks and their clients. While banks have choices to make in terms of routes to pick (facial, voice, Iris, fingerprint etc.), uni-factor vs. multi-factor, they also need to decide on the preferred implementation options that could be in-house, cloud-based or a combination of both with the data being in-house for security reasons. We also believe that biometrics will eventually move from external body traits to internal traits like heart rate or vein recognition that offer higher level of security cover. Then there is the option of behavioral biometrics that looks at the gestures and speed with which users type their passwords (for example) and then combine these with traditional biometrics to offer a more robust solution. These surely are exciting times for banks, customers and technology providers.

About the Author

Anirudh Jayaraman is the Practice Partner for Digital Banking and Channels. Anirudh, who has been with Wipro for a decade now, leads multiple large-scale digital banking initiatives across North Americas and Europe.

About Wipro

Wipro Ltd. (NYSE:WIT) is a leading information technology, consulting and business process services company that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology." By combining digital strategy, customer centric design, advanced analytics and product engineering approach, Wipro helps its clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, Wipro has a dedicated workforce of over 160,000, serving clients in 175+ cities across 6 continents. For more information, please visit **wipro.com** or write to us at **info@wipro.com**

DO BUSINESS BETTER

CONSULTING | SYSTEM INTEGRATION | BUSINESS PROCESS SERVICES

IND/PMCS/JUN2016-DEC2016