BIZCOMMUNITY

Open banking puts customers in charge

By Yogesh Mathur

29 May 2019

Could open banking usher in a new era of convenience, access and service differentiation? It's a tantalising possibility, but not one without potential security pitfalls which must be closely managed and mitigated. Done properly, concept of open banking can benefit all bank customers with improved services which can result from meaningful collaboration.

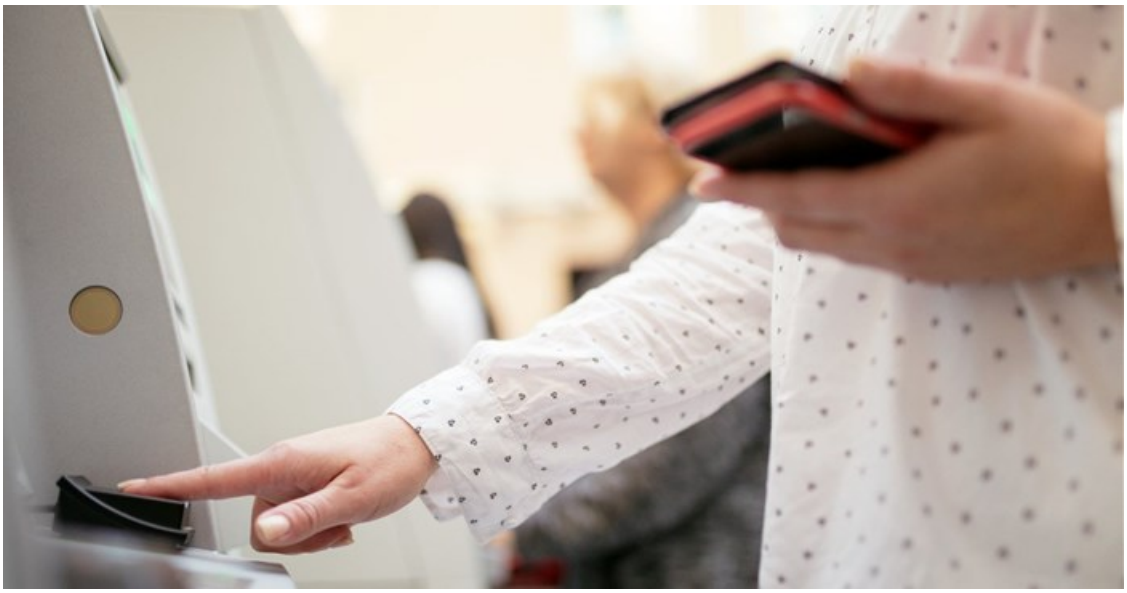

Image source: Getty/Gallo

Open banking essentially describes the practice of banks sharing customer information – that is, your information – with trusted third parties for the creation of additional services. With your consent, these third parties can access reams of financial data, such as transaction history and spending behaviour, which was, until now, held solely by the banks.

Just who are these third parties? There is a growing industry of fintech innovators seeking to revolutionise various aspects of banking, and with open banking, established financial institutions are able to partner with these innovators.

Parallel developments

Already, customers are becoming increasingly receptive to alternative payment methods from ‘non-financial’ companies, including Apple Pay, Samsung Pay, Amazon, and Google; while Apple Pay is not available locally, others are and that includes the likes of PayPal (one of the founders of which, Elon Musk, is South African-born) and Bitcoin.

These solutions, along with multiple parallel developments like smartphones, social media and more, are teaching consumers to demand everyday information instantaneously and with little effort – and now consumers want the same sort of control over their money. That's where open banking comes in. People recognise that when their information is shared, amazing things can happen (Google's context-awareness is a good example of this in practice).

But, people are also aware than potentially bad things can also happen. There is a 'creepy' element and there is most certainly a 'criminal' element, given the type of information banks hold. Therefore, as open banking increases in popularity, it is imperative that end-users are safeguarded from identity theft and data breaches

The scale of the risk to banks is clear: when Gemalto conducted a survey of 11,000 digital and mobile banking consumers across 14 markets, we found that, 49% of customers would switch their bank if their current bank had experienced a security breach and 52% would switch to a provider with more rigorous measures.

So, regulation calling for greater security and control is, in general, a sensible move in line with what the market is doing anyway.

Mitigating risk

Mitigating risk depends on the use of multiple technologies, such as biometric software, government ID document readers, and identity and access management (IAM) solutions. These all support the secure transition from traditional to open banking interactions. Users can look forward to a secure environment, delivering identity verification, user authentication, transaction verification, and fraud prevention to create a seamless user experience, regardless of device.

Machine learning, and artificial intelligence routines can be used to develop personalised authentication profiles for individuals, creating personalised authentication scenarios. Ultimately, machine learning creates a personalised risk assessment for each individual, with each authentication need. For example, if there are no suspicious activities for a given user when conducting a transaction, the individual will receive less authentication requests. The process allows a person to be identified and authenticated based on a set of recognisable and verifiable data, which are unique and specific to them, creating a more seamless and secure user experience.

The provision of a secure environment is not simply a response to user requirements but is also a regulatory obligation. We have seen a sharp rise in cyberattacks and breaches, and the financial services sector is a particularly hot target given the assets it holds.

Biometrics

Biometrics remains a key part of the multi-factor authentication mix. Biometric technology as a means of authenticating identity is on the rise and form an integral part of a broader multi-factor set of authentication credentials. By this we mean that it can play the role of "something you are", and then you need "something you know" – a passphrase, for example – and something you have, like a physical token. For many relatively low-value transactions, it may well be that a simple biometric reading alone would be sufficient, but if you hit certain thresholds you might trigger a second.

It's likely that a growing number of banks are planning to offer more biometric solutions to their customers; we've already seen the introduction of biometric ATM machines. Gemalto research indicates that a high proportion of banks plan to implement fingerprint scanning as well as face, voice and iris (eye) recognition

Adopting an agile approach

Customers are becoming increasingly demanding with increasing expectations from technology. To be truly satisfactory, the digital banking experience needs to go far beyond user friendliness and responsiveness. The expectation is not only to access core services such as bill payment and transfers but to tap into associated products and services such as loans, saving plans and investment.

Open banking provides an opportunity for innovation in a fast-evolving sector. Banks are adopting an agile approach and are focused on utilising mechanisms to create a new set of customer experiences delivering no only security but convenience. Fintech start-ups are already trying in this vein, using real-time transaction data to build up a careful profile of each customer and offering other, secure, transaction options to customers.

Open banking appears to offer many positives, however, regulators must be careful, as it is not without other risks. The second Payment Services Directive (PSD2) was recently implemented in Europe and is responsible for ensuring that banks adhere to rules and regulations around open banking. This was a significant move for the payments industry as access to this information will help new entrants create innovative new products and services and ultimately better serve the consumer.

However, in South Africa, open banking – while attracting the interest of some of the major banks hasn't yet been mandated by local regulators.

With a global transformation towards open banking underway, strong authentication standards are needed to deliver the promises of open banking and a careful balance between fighting fraud and keeping consumers happy must be struck.

ABOUT THE AUTHOR

Yogesh Mathur is the vice president for sales, telecom and banking at Gemalto