Biometric authentication

Creating a strategy that works for financial institutions and their customers

By Charlie Jacco

Financial institutions are no strangers to biometrics, but they're showing new interest in this technology, for good reason. Passwords have long been known as a flawed method of authentication. Many people still use the same password on several websites, making it easy for cybercriminals to steal their identity. To counteract that, financial institutions (FIs) leverage multi-factor authentication such as one-time passwords sent over SMS or email, but customers find the process onerous. In response, biometric authentication using facial, fingerprint and voice recognition, as well as other biometric techniques and technologies, is on the rise worldwide.

To maximize customer retention and revenue, financial institutions are avoiding a one-size-fits-all approach. That means letting clients create a personalized experience, based on a specific security policy that includes biometrics, so banking is safer and easier on any device. In a digital age where personal relationships matter less — people seldom talk to their bankers anymore — it's crucial to building brand loyalty.

Why biometrics are here to stay

Biometrics are becoming more affordable to leverage, and banks have been enthusiastic adopters. For example, Bank of America recently teamed up with South Korean electronics giant Samsung to develop technology that lets customers access its mobile banking app by using a photo of their eye.[1] In China, HSBC clients can do the same by blinking at their phone's camera in selfie mode.[2] Commonwealth Bank of Australia now supports the iPhone X's Face ID feature,[3] as do Britain's Lloyds Banking Group and Nationwide.[4]

In biometrics, financial institutions see a way to shield themselves from the significant losses that a data breach could bring. They're less worried about broader attacks — such as hackers using a false login page to obtain passwords and steal a large sum of money — than identity theft fraud and breaches that defeat their security technology.

That's because banks face so much competition in the wider fintech space, from alternative payment methods that may have nothing to do with them. During the next

[1] http://www.biometricupdate.com/201709/bank-of-america-exploring-use-of-iris-facial-recognition-technologies
[2] http://www.biometricupdate.com/201710/hsbc-introduces-facial-recognition-to-its-mobile-banking-app-in-china
[3] http://www.zdnet.com/article/commonwealth-bank-launches-facial-recognition-login-for-iphone-x/
[4] https://www.macrumors.com/2017/11/01/uk-banking-apps-face-id-support/

two years, between fintech upstarts and new European Union regulations that allow public application programming interfaces (APIs) in banking,[5] rivalry will be fierce. For banks, this means ensuring that customers perceive dealing with them as safe and easy.

Letting the customer decide

Here's where biometrics come in — and where banks need to find the right balance.

Over the past decade, clients have grown used to having multiple security factors associated with their accounts.

Two-step authentication is more secure but still vulnerable to hackers, and customers view it as burdensome, so the trend with mobile devices is to leverage thumbprint readers or selfie pictures. This relies on two assumptions: that customers are using a mobile app — and are comfortable doing so.

Banks are realizing that the best approach is allowing customers to pick and choose from many options, and allow that experience to carry across multiple digital channels, creating a unique omni-channel experience. Take the next generation of automatic teller machines (ATMs), called intelligent teller machines, or ITMs. When a client interacts with an ITM, they can receive a message on their mobile phone asking if they want to withdraw money. One person might be okay to withdraw US$200 by sticking their thumbprint on the phone and telling the ITM how much, but for larger sums they want the physical sensation of inserting a card and entering a personal identification number (PIN). A younger customer may be comfortable using an iris scan reader to authenticate their identity.

In private banking, some institutions now identify clients by adding their voiceprint to the mix, plus the unique biometric tremble they exhibit while holding a phone.

Privacy matters

For banks, striking a balance means finding a happy medium between their security posture and the security experience they want to deliver. That includes following privacy rules, especially in the EU,[6] for gathering biometric and other information from customers. It helps to be clear on what a bank can take without a client's consent or knowledge, and when it must ask permission.

Looking beyond mobile devices, financial institutions can choose from dozens of biometrics vendor products — for now, anyway. In the next 12 to 18 months, the market will consolidate dramatically as big players gobble up vendors and offer their wares as part of solutions.

No matter what technology they use, banks should consider making biometrics part of a holistic approach to security that lets clients personalize the customer experience.

[5] https://www.bloomberg.com/news/articles/2017-10-23/european-banks-will-have-to-share-data-with-their-rivals

[6] https://www.itgovernance.eu/blog/en/gdpr-things-to-consider-when-processing-biometric-data/

Contact

Charlie Jacco
Financial Services Advisory Partner and Cyber Security Lead
KPMG in the US
T: +1 212 954 1949
E: cjacco@kpmg.com

kpmg.com/socialmedia

Designed by Evalueserve.

Publication name: Biometric authentication

Publication number: 135156a-G. Publication date: January 2018