5. Behavioural biometrics, a step further in digital identification for financial services

Growth of biometrics in the banking industry

As the world becomes more digital, financial institutions need to keep up with consumer demands. The use of biometrics in the banking industry has been gaining traction thanks to the arrival of devices that already include biometric readers and the expansion of wearable banking. The increasing scale and frequency of cyber attacks against user accounts in the past few years has shown that security cannot rely on identification means based solely on static biometric elements that can be compromised. Behavioural biometrics could be a solution to combating fraud and identity theft.

Passwords versus Biometrics

As a result of poor user experience, high and rising costs[20] and security breaches associated with the use of passwords, banks have been migrating to new digital identification systems that meet both the objectives of ensuring secure identity and improving user experience.

Biometrics is not uncharted territory for the financial industry; banks have explored options such as fingerprint scanning for decades, but the convenience and proliferation of mobile devices are making biometrics accessible to virtually anyone with a smartphone.[21] According to Goode Intelligence[22], by 2020 there will be at least 120 million customers using mobile biometrics on a daily basis for their financial transactions.

Biometrics use

There are two main types of biometric identifiers: **i)** physiological or static characteristics, based on the shape or composition of the body (fingerprints, iris, palm veins, face) and **ii)** behavioural characteristics, based on a person's behaviour (keystrokes, mouse movements, hand-eye coordination, hand tremors, navigation, scrolling and other finger movements).

Although financial institutions have been introducing different static biometrics for identification, **at present, fingerprint recognition systems are most widely used.** According to Deloitte[23] there will be one billion smartphones with fingerprint readers in use by the end of 2017. Nevertheless, by 2018, iris and face recognition will start to rival fingerprints. For instance, BBVA has recently started using biometrics for remote account opening in Spain, by verifying the customer's identity through a face recognition process. In India, project Aadhaar has captured graphic and biometric data of a billion residents in the largest biometric project of its kind in the world.

20: A recent survey of US companies found that each employee loses, on average, $420 annually grappling with passwords
21: Source: Biometrics: the future of Mobile Payments. Nathaniel Karp, BBVA Research, July 2015.
22: Source: Mobile Biometrics for Financial Services; Market & Technology Analysis, Adoption Strategies & Forecasts 2015-2020. July 2015.
23: Source: A world beyond passwords: Improving security, efficiency, and user experience in digital transformation. Goode Intelligence. December 2015

Security issues

Hackers have figured out how to replicate the traditional means of authentication (SMS codes, tokens). Although static biometrics are relatively secure due to the fact that physical attributes are unique, it is also true that physical characteristics are **public, we cannot hide them and therefore they are easy to recreate and reuse.** Recently, we have seen in the news that hackers had tricked facial-recognition logins with photos from Facebook. In Japan, The National Institute of Informatics (NII) is warning that fingerprint recognition technology is allowing hackers to copy patterns from photos of people giving the peace sign. The consequences of a false positive can be very serious. Furthermore, when our biometric data is compromised, it cannot be used again and the damage is permanent.

Adoption of behavioural biometrics

Behavioural biometrics technology is able to learn patterns in user behaviour in order to build an identification model. The software analyses the way users interact with the different devices (phone, PC, tablets), how they hold the mouse, make keystrokes, how quickly they move, the pressure with which they hold the phone, etc. Over time, these biometrics are interpolated through algorithms and are able to define a unique pattern of each user in order to determine his or her identity in a certain way.

One element that differentiates this technology from static biometrics in verifying identity is that **the data is collected in a passive way and it does not interrupt the user activity, a key element for the user experience**

Companies like Google, with Project Abacus, are developing machine learning to authenticate users based on multiple assessments of their behaviour. The use of sensors, such as the camera, accelerometer, and GPS functions, allows smartphones to obtain a wide range of information about users, including their habitual geolocations, and how they type, walk, and talk.

Some banks have started to embrace behavioural biometrics as a replacement for passwords on mobile devices. One such bank is Leumi bank, an Israel-based bank that monitors users' finger size and the pressure of the user's touch to enable passive authentication. Some Fintechs, such as Mobetize, have also adopted behavioural biometrics to analyse the patterns of users and determine whether they are genuine customers, bots or hackers.

Legal Issues

As biometric technology is so new, there are **very few regulations that specifically address its use and application**. The biggest risk in the use of static biometrics relates to privacy issues, as readings are often stored in databases that can be compromised.

In Europe, regulators recognise that these technologies could improve user experience, but could also "lead to a gradual loss of privacy if no adequate safeguards are implemented"[24]**.** The new General Data Protection Regulation establishes that, for the processing of "special categories of personal data" such as biometrics, a higher level of user

24: Source: Data protection working party, Opinion on developments in biometric technologies, April 2012

consent – “explicit” consent - is required. Directives such as the new Payments Services Directive (PSD2) establish two-factor authentication for certain payments, where the use of biometric identification methods can increase the acceptance of mobile payments. The eIDAS Regulation calls for the optional use of biometrics to support eSignature applications throughout the EU. In the USA, some states have instituted regulations to protect the privacy of individuals’ biometrics.

In the case of behavioural biometrics storage, as human and interaction signals are collected, instead of physical biometrics, it is significantly a more privacy-friendly method.[25]

Conclusions

It is expected that banks will increase the use of these technologies, as they are becoming more accurate and easier to integrate into online and mobile applications. As single authentication methods are clearly vulnerable to attacks and it is where most of the fraud is taking place today, **banks are introducing behavioural biometrics as an additional way to protect the identification process. This approach allows the detection of anomalies in a customer’s patterns of usage after the authentication. It is the so-called multi-factor authentication.** By monitoring the patterns in a continuous way within a session, behavioural biometrics offer an integral solution to protect accounts from being taken over by hackers. The other factor that makes biometrics based on behaviour so attractive is user experience, as it works without interrupting the user’s daily activity in any way.

25: Source: Biometrics: The Physical Attributes vs. Behavioral Patterns Privacy Debate

DISCLAIMER

This document has been prepared by BBVA Research Department, it is provided for information purposes only and expresses data, opinions or estimations regarding the date of issue of the report, prepared by BBVA or obtained from or based on sources we consider to be reliable, and have not been independently verified by BBVA. Therefore, BBVA offers no warranty, either express or implicit, regarding its accuracy, integrity or correctness.

Estimations this document may contain have been undertaken according to generally accepted methodologies and should be considered as forecasts or projections. Results obtained in the past, either positive or negative, are no guarantee of future performance.

This document and its contents are subject to changes without prior notice depending on variables such as the economic context or market fluctuations. BBVA is not responsible for updating these contents or for giving notice of such changes.

BBVA accepts no liability for any loss, direct or indirect, that may result from the use of this document or its contents.

This document and its contents do not constitute an offer, invitation or solicitation to purchase, divest or enter into any interest in financial assets or instruments. Neither shall this document nor its contents form the basis of any contract, commitment or decision of any kind.

In regard to investment in financial assets related to economic variables this document may cover, readers should be aware that under no circumstances should they base their investment decisions in the information contained in this document. Those persons or entities offering investment products to these potential investors are legally required to provide the information needed for them to take an appropriate investment decision.

The content of this document is protected by intellectual property laws. It is forbidden its reproduction, transformation, distribution, public communication, making available, extraction, reuse, forwarding or use of any nature by any means or process, except in cases where it is legally permitted or expressly authorized by BBVA.

BBVA | Research

This report has been produced by the Digital Regulation Unit:

Chief Economist for Digital Regulation Unit
Álvaro Martín
alvaro.martin@bbva.com
+ 34 91 537 36 75

María Álvarez
maria.alvarez.caro@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Edward Corcoran
Edward.corcoran@bbva.com

Jesús Lozano
jesus.lozano@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Ana Isabel Segovia
ana.segovia@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

BBVA Research

Group Chief Economist
Jorge Sicilia Serrano

Macroeconomic Analysis
Rafael Doménech
r.domenech@bbva.com

Global Macroeconomic Scenarios
Miguel Jiménez
mjimenezg@bbva.com

Global Financial Markets
Sonsoles Castillo
s.castillo@bbva.com

Global Modelling & Long Term Analysis
Julián Cubero
juan.cubero@bbva.com

Innovation & Processes
Oscar de las Peñas
oscar.delaspenas@bbva.com

Financial Systems & Regulation
Santiago Fernández de Lis
sfernandezdelis@bbva.com

Countries Coordination
Olga Cerqueira
olga.gouveia@bbva.com

Digital Regulation
Álvaro Martín
alvaro.martin@bbva.com

Regulation
María Abascal
maria.abascal@bbva.com

Financial Systems
Ana Rubio
arubiog@bbva.com

Financial Inclusion
David Tuesta
david.tuesta@bbva.com

Spain & Portugal
Miguel Cardoso
miguel.cardoso@bbva.com

United States of America
Nathaniel Karp
Nathaniel.Karp@bbva.com

Mexico
Carlos Serrano
carlos.serranoh@bbva.com

Turkey, China & Geopolitics
Álvaro Ortiz
alvaro.ortiz@bbva.com

Turkey
Álvaro Ortiz
alvaro.ortiz@bbva.com

China
Le Xia
le.xia@bbva.com

South America
Juan Manuel Ruiz
juan.ruiz@bbva.com

Argentina
Gloria Sorensen
gsorensen@bbva.com

Chile
Jorge Selaive
jselaive@bbva.com

Colombia
Juana Téllez
juana.tellez@bbva.com

Peru
Hugo Perea
hperea@bbva.com

Venezuela
Julio Pineda
juliocesar.pineda@bbva.com

CONTACT DETAILS: BBVA Research: Azul Street, 4. La Vela Building - 4 and 5 floor. 28050 Madrid (Spain). Tel.:+34 91 374 60 00 y +34 91 537 70 00 / Fax:+34 91 374 30 25 - bbvaresearch@bbva.com www.bbvaresearch.com