print images from a distance? Kits are openly available on the internet that allow you to 'lift' someone's fingerprint and make a simple silicon mould of it, which can fool many sensors, and fingerprints have been captured from three metres away with suitable equipment[7]. Such attacks are potentially more serious than credit card skimming, for example, because fingerprints cannot be re-issued or reset.

So how common are such attacks likely to become, and therefore how much fraud will take place? We need to know the associated cost of fraud per user per year, as illustrated in Table 1. Figures X and Y are already well-known to financial institutions. Z is currently unknown, although expected to be low. Therefore a sensible next step is to run a pilot study using such a system. If the trials show that the number of fraudulent transactions significantly exceeds those in existing systems then it is 'back to the drawing board'. If fraud is reduced, the technology may become more widespread. Pilot programmes using Touchless ID technology are already in the works to quantify this unknown, and to date there have been no known cases of fraud.

In conclusion, fingerprinting has proven to be a reliable and effective identification tool. So its evolved technical applications – including new solutions like Touchless ID – will likely continue to be central players in the biometrics field. If biometric fingerprinting is used as expected, the time we all spend trying to remember passwords will be saved, authentication will become simple and fraud should be reduced.

About the author

Dr Francis Mather is a tech visionary with a deep knowledge of optics. He leads the computer vision and liveness detection efforts at Veridium. He has over 15 years of experience in research and technology management, translating creative thought into working solutions. Before Veridium, he was the principal researcher at Sharp Corporation's European lab, where he pioneered the world's first dual-view display, now used by Toyota and Jaguar Land Rover. He was elected a Fellow of the Institute of Physics in 2014, and earned his PhD in Physics from the University of Exeter.

References

1. 'Jaamehol-Tawarikh' (Universal History), attributed to Khajeh Rashiduddin Fazlollah Hamadani (1247-1318).
2. 'Biometrics Technology Market By Technology – Growth, Share, Opportunities & Competitive Analysis, 2015-2022'. Credence Research, April 2016. http://www.credenceresearch.com/report/biometrics-technology-market.
3. 'Death of the Password'. Gigya Inc, 2017. http://www.gigya.com/resource/whitepaper/death-of-the-password/.
4. Bhagavatula, Chandrasekhar, et al. 'Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption', 2015.
5. Tim Stevens. 'Ice Cream Sandwich face unlock demo'. Engadget, 19 October 2011. Accessed January 2017. http://www.engadget.com/2011/10/19/ice-cream-sandwich-face-unlock-demo-video/.
6. 'Hoyos Labs Joins National Research Program to Inform Creation of Contactless Fingerprint Technologies for Federal Agencies'. Veridium, 16 February 2016. Accessed January 2017. https://www.veridiumid.com/biometric-authentication-company/press-releases/hoyos-labs-joins-national-research-program-inform-creation-contactless-fingerprint-technologies-federal-agencies/.
7. Brett Williams. 'Japanese researchers: your peace-sign selfies are putting you at risk'. Mashable UK, 11 January 2017. Accessed January 2017. http://mashable.com/2017/01/11/stolen-fingerprints-peace-signs/#fCePwWeePmql.

Selfie banking: is it a reality?

Steve Cook, Daon

Steve Cook

The progression of digital banking is changing the face of the banking sector completely. One key factor driving this change is digital identity assurance in the form of biometric technology. But this in turn has created a significant challenge. Most traditional banks have old legacy systems and making the digital transformation leap is almost like building a completely new bank while still servicing existing customers and attracting new ones.

This challenge comes at a time when banks are facing multiple other pressures, including legislative change and the threat of new competition. There has also been an explosion in mobile banking. A recent study from Deloitte[1] highlighted that 43% of adult smartphone users in developed countries are using their mobile device to check their bank accounts, and this is likely to increase significantly in the coming few years. Meanwhile, traditional banks are competing with many new start-up providers, collectively known as 'challenger banks', entering the arena. Over 30 new banking licences have been issued in Europe in recent years and many more applicants are awaiting approval.

The key advantage that these new digital banks have is that they are nimble, with a very low cost base and are also technically more advanced. The majority only have an online or mobile presence,

giving them the flexibility to introduce new customer-facing, user-friendly features and products. They are also connected into the world of social media and can deliver speed-to-market. In contrast, many traditional banks are slow to respond to new market trends: their systems just cannot adjust as easily as starting afresh. So even though the majority of big banks do not seem to be overly concerned with these start-ups, they cannot afford to be complacent. Keeping pace with these new fintech innovators should be a priority for all banks because many of them are leading the way with customer service.

In addition to the technological revolution that is transforming banking, a series of new regulatory guidelines are coming into force. These include renewed European directives such as the EU's new data privacy directive, called the GDPR, the Fourth Anti-Money Laundering directive and the Payment Services Directive 2 (PSD2), all of which are designed to improve our online security.

PSD2 is the most critical of these developments for banks, because they have only a very short timeframe in which to implement the required changes. The current status is that the European Banking Association (EBA) is considering responses to the PSD2 consultation process, which is expected to be completed by May 2017. The final guidelines will then be published in summer 2017. The full guidelines will apply from 13 January 2018 and therefore need to be followed for all authorisations granted from that day onwards. In banking lifecycles, that is just the blink of an eye.

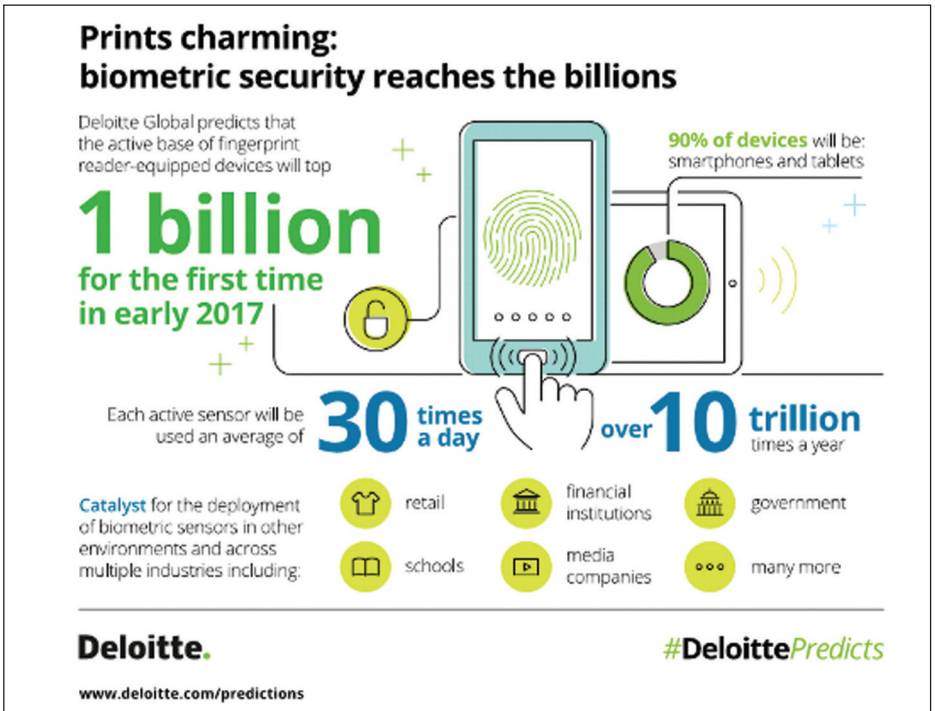
One of the most critical sections of PSD2 is known as 'Secure Customer Authentication'. SCA is an important regulation for securing payments that will affect all finance service providers. It will demand a more stringent, two-factor authentication process, requiring two of the three factors set by the EBA guidelines (which have to be independent of each other), namely:

1. Something you know – a pin or password or something else the customer might know, otherwise known as KBA (knowledge-based authentication).

2. Something you have – your device, such as a mobile smartphone.

3. Something you are – an identifier Inherent to you, like a biometric credential.

Crucially 'something you are' is going to be where new digital technology will assist with the identity verification process. In terms of biometric authentication, this could be via iris, face, voice, palm, vein, gesture, thumb or fingerprint identification. A few banks and lenders have begun to introduce modalities such as face, voice and fingerprint recognition to give customers a more convenient way to check their account balance or make payments. Eye



The number of active fingerprint reader-equipped devices has just topped 1bn, says Deloitte, with 90% of them smartphones and tablets.

print and behavioural patterns are also being adopted, while iris, vein and gesture recognition are likely to be used in the future. This depends on whether new devices will have the hardware capabilities to recognise these modalities.

Specifically, a number of banks have already enabled Touch ID on the latest Apple iPhone models for some of their customers. However banks do not control the Apple protocols as these are stored on the user's device. This is not as secure as if financial service providers had a server-based identity management system whereby they could fully manage the risk of fraudulent activity. Banks need to ensure they have control of the identity of their customers in order to secure logins and transactions. Using more than one biometric method in real time (known as a step-up process) will reduce the risks significantly.

Advantages

Clearly, there are several reasons why banks should use biometric technology. It helps to improve the user experience, by providing a simple process to verify existing customers or to enhance KYC (Know Your Customer) on-boarding methods. Customers can create their own set of biometric credentials and then use a combination of these biometrics to log in, verify their accounts and authenticate transactions. As consumers become more familiar with digital channels, banks will increasingly need to use digital means of customer identification, in order to be able to remotely on-board and authenticate customers while complying with regulatory requirements.

Research shows how quickly consumers are moving to digital channels and biometrics. A 2016 survey of 4,000 consumers by Gigya found that 80% of those expressing a preference felt biometrics was more secure than traditional usernames and passwords[2]. Today, almost the same percentage of consumers currently use a thumb or fingerprint to unlock their smartphones. According to research from Visa[3], almost twice as many British consumers (60%) are likely to trust banks to store and safeguard their biometric information than they are government agencies (33%). Meanwhile, Acuity Market Intelligence projects that by 2020, global mobile biometric market revenues will reach $34.6bn annually[4] while another study from Deloitte predicts there will be over 1bn devices globally with biometric-enabled security in 2017[5].

So what about 'selfie banking'? Many experts predict that paying for goods and services with a selfie will become a more standardised method than currently using the fingerprint on your smartphone. This is because facial recognition is a more reliable form of biometric check than a fingerprint. If facial recognition is combined with other modalities such as voice, iris or a fingerprint, then this raises the level of certainty and confidence.

In addition, biometric authentication has advanced to the extent that it offers additional security based on liveness functionality. For example, to prevent spoofing, a customer using their face as a biometric credential may be asked to perform a task such as blinking their eyes, nodding their head or speaking a random