Hybrid tech: the future of biometric ID verification?

Philipp Pointner

Philipp Pointner, Jumio

Identity fraud is a significant threat. In the UK, for example, it is now the largest category of fraud carried out against individuals, with an estimated 3m victims and a cost of £5.4bn[1] annually. Little wonder then that consumers are putting more pressure on businesses to adopt biometric solutions to tighten security procedures when on-boarding and verifying new customers[2].

In the financial services sector, NatWest[3] and Visa[4] have been working with biometrics providers to improve both security and consumer experience. McDonalds[5] is also considering biometrics for employee security and access rights and Uber[6] has launched a facial recognition software service for drivers to authenticate themselves. Equally, for travellers to the US, fingerprint scanning at airports is a common experience and iPad and iPhone users will be familiar with using fingerprints to unlock their devices and making payments on ApplePay via fingerprint authentication. Evidently, as consumers, employees and citizens, biometrics are becoming increasingly common in our lives. Yet despite this rise in popularity, there remains some debate as to whether biometrics truly represents the future of identity verification. After all, as long as fingerprints can be tampered with, facial scans compromised and voice recognition manipulated, concerns will remain regarding biometric technology's potential to tackle identity fraud and comprehensively verify customer ID.

"For all its potential, there is still one critical flaw with biometric technology: while it can verify an identity, it cannot establish it"

Continued instances of fraudulent transactions, hacks and breaches have created a pressing need for better ways to verify consumers. So as an industry, our mission must be twofold: to create a transaction environment that minimises the likelihood of identity fraud; and to improve the consumer experience while doing so. This article provides an overview of how today's biometric technology is being used in identity verification, its critical flaws and how, when combined with other technologies, biometrics can ensure a stronger future of ID verification.

Panacea or problem?

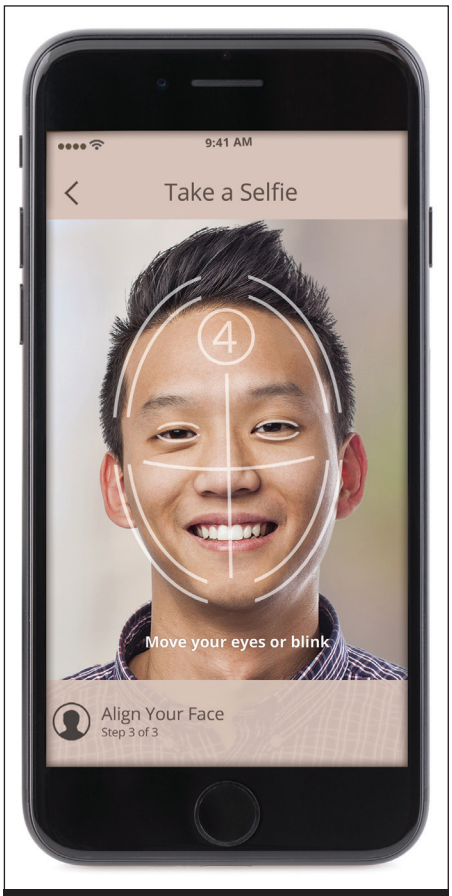
Biometrics is simply the process of using unique human characteristics to verify unique identity; and of course the concept is nothing new, having first emerged in the 19th century when fingerprint identification was used to solve crimes. But with the advent of the digital age, biometrics have become increasingly visible in multiple contexts, and the global market is expected to reach a value of $30bn by 2021[7]. Enthused by the potential of biometrics to deliver both a convenient user experience and watertight security, businesses – most notably financial services – have been quick to see it as a panacea for their problems. But if this were true, every verification and authentication process would merely involve a quick iris or fingerprint scan. In fact, each of the different biometric-based verification methods currently being developed and rolled out has clear advantages and disadvantages:

- Voice recognition can verify someone in around 15 seconds, quicker than passwords[8]. Yet its accuracy is still open to question. For example, can it recognise a voice alongside background noise? Equally, in terms of security and user experience, would individuals always be fully comfortable using voice recognition in a public place?
- Facial recognition – also known as 'selfie' verification – offers a quick, convenient scan suited to the digital age. However there are still limitations. Many ID verification solutions require lighting to be of a certain standard or a photograph to be of sufficient quality to be recognised. Again, either by accident, nature or design, facial features can change and the ability of facial recognition software to adapt to this is not sufficiently robust in many cases. Most importantly, a facial recognition scan can be spoofed if live detection technologies are not in place. A fraudster may simply hold up a picture of the victim and proceed uninhibited.
- Fingerprint recognition is widely used, simple and trusted. But it is not perfect. Fingerprints can be copied or manipulated. Recent research suggests that fraudsters can even easily re-create fingerprints from selfies, especially those containing two-finger 'peace' signs and other poses that expose the fingertips[9].

Challenges to establishing identity

For all its potential, there is still one critical flaw with biometric technology: while it can verify an identity, it cannot establish it. At some point in their relationship with a business, customers have to be able to submit the biometric details to the company with proof that those details are valid and authentic. In fact, any sector that involves the transfer of money, such as financial services or online gaming, will have strict know-your-customer (KYC) and anti-money laundering (AML) requirements. These businesses have to know that a new customer is who they say they are. The new customer has to be able to present some sort of government-issued identification in order to verify their identity.

But Jumio research into mobile abandonment across a number of industries has found that, in the online gaming industry, 24% of



Netverify: an example system that combines biometric facial recognition and liveness detection technology to prove cardholder presence.

attempts to register for a new account were abandoned and, for financial services, 25% of attempts to open a new account were abandoned. The research looked in more detail at what was happening with online account opening in the banking industry and discovered that KYC and AML requirements meant that 30% of online applicants still had to go to a branch with a physical ID in order to complete the process. As a representative of one bank said: "We require the customer to provide three things: proof of identity, proof of address and proof that they are who they say there are. This is far more difficult to do online."

This brings home the critical factor relating to ID verification – in order to access any service that has KYC and AML compliance requirements, the customer has to be able to prove they are who they say they are. This is a problem that biometrics alone cannot solve.

Biometrics plus

A golden rule of authentication and security is that the more layers there are, the more secure it is. Data from Visa shows that 73% of customers view biometric technology as a secure way of verifying an account holder's identity when used together with another security protocol[10]. That's why banks will often require a mixture of password and PIN to access online services and why, on the iPhone for example, the biometric fingerprint ID security is enhanced by submitting a passcode each time the phone is turned on. Multi-factor authentication is becoming the norm.

For KYC and AML purposes, biometrics can still have a critical role to play. This is especially true when considering the PSD2 (Payment Services Directive) and 4th EU Money Laundering Directive. For example, the European Banking Authority's Regulatory Technical Standards (RTS), which were mandated under the revised PSD2, require strong customer authentication and common and secure communication. The aim is to enable an open and secure market in retail payments across the European Union, sustained by a strong verification system. There will be two exemptions from the RTS: one based on transaction risk analysis linked to a pre-defined level of fraud; and the other for payments at 'unattended terminals' such as rail ticket machines. In addition, all consumer transactions of over €30 that are not covered in these exemptions must meet strong authentication requirements, which, unless enabled with quick and easy-to-use secure technology, could threaten to create barriers to conversion for online sales.

However, while authentication can establish an identity, it cannot confirm it. For example, passwords are commonly used as part of a strong authentication system. But what happens when a customer forgets the password or if that password is stolen? On this basis, strong verification procedures can strengthen, for example, a bank or payment service provider's authentication measures and ensure that authentication assistance only reaches the owner of the account.

"A fully comprehensive approach to identity verification demands the combination of technology, automation and human agents as identity experts. This dynamic framework includes machine learning, computer vision and biometric facial recognition"

Meanwhile, the 4th EU Money Laundering Directive (MLD), which came into full effect in Europe in July 2017, requires regulated firms to verify customer identity or face hefty penalties for non-compliance. It mandates ID document verification to open digital accounts, as part of co-ordinated efforts to curb large-scale money laundering practices and boost the safety of high-risk, high-value industries. This affects credit institutions, financial institutions, auditors, legal professionals, trusts, estate agent and gambling operators. When the onset of PSD2 and 4th EU MLD are combined with the knowledge that different markets have their own precise and specific KYC and AML requirements, it becomes clear that companies across various

A multi-layered approach to ID verification. This shows the user journey from selecting a document type and country, to taking a scan of the document and finally establishing biometric facial recognition via a selfie.