David Poole explores the changing face of ID verification and examines the importance of the PIN

VERIFYING IDEN DIGITAL AGE

©Getty Images

Identity and verification are two linked but subtly different concepts that in the advent of the digital age are changing and evolving to match the requirements of digital commerce. Verification is answering the question: "Is this person who they say they are?", while identity systems seek to distinguish an unknown person based upon the evidence that they provide. As an example, a passport will identify someone, entering a debit card into an ATM will identify an account, while entering a PIN number when making a withdrawal from an ATM will verify them.

Identity and verification have been a part of our day-to-day lives for generations. Even before the electronic age, passports were needed to enter a country and signatures were required to make bank transactions. Yet all of these methods required the presentation of a physical document. Until the online revolution, the majority of transactions were carried out face to face.

The online revolution, however, has changed the face of commerce utterly. With an estimated 1.61bn online shoppers globally, and £52.25bn spent via e-commerce in the UK in 2015, the last decade and a half has seen e-commerce grow from a niche challenger to the dominant platform for global business. E-commerce itself has evolved during this period as consumers have moved increasingly from desktop to mobile as smartphones and tablets have increasingly become the platform of choice for buying products and services remotely.

TITY IN THE

Fingerprint recognition is far from perfect and prints can be copied by fraudsters using chemicals

"The rise across all fraud loss types during 2015 owes much to the growth of impersonation and deception scams, as well as sophisticated online attacks such as malware and data breaches."

Today the ability to shop and transact online no matter where we are is something that's taken for granted. It has brought new levels of convenience to our lives. Yet this convenience has not been without cost and this cost is the increasing challenge of managing identity and verification in a manner that is both secure and doesn't impact on the user experience to a detrimental level.

Online commerce always requires authentication and because, by and large, physical documents cannot be used online, it is the challenge of managing this in a secure manner that is one that has perplexed merchants, security providers, banks and all stakeholders in digital commerce.

Despite the challenges remote identity and verification may bring, it isn't in itself anything new. Consumers have carried out transactions by mail or telephone (MOTO) for decades. Yet these all relied on forms of authentication such as address and date of birth. Given that this information is freely available online, it is no longer fit for purpose as a secure method of verification. This has driven a need to develop and accept new methods of authentification with both customers and businesses having to adapt to the new business realities.

Among currently used methods, the first to come to mind is the password, which has its own drawbacks. Passwords rely on end users playing their part in keeping them secure. This means using complex passwords with a mixture of letters, numbers and symbols, and changing them frequently, making them hard to guess. As we know, this rarely happens and lax end-user security is all too often to blame for hacks and breaches. That isn't to say that the password doesn't have an important role to play in identity and verification but, on its own, it is not secure enough. What then can we expect from the next-generation of post-password authentication?

Machine learning is a branch of artificial intelligence study that concentrates on induction algorithms and on other algorithms that can be said to 'learn'. This discipline – which currently has a wide variety of applications in the digital world – has considerable possibilities in the sphere of authentication.

Taking the use of mobile as an example, each of us has our own individual quirks in how we use our handsets. We will hold it in a certain way, enter keystrokes in a particular way and have certain unique ways in which we interact with specific apps. All of these can be 'learned' by an intelligent mobile device, which can then tell if the person using the handset is the same person that should actually be using it.

Machine learning – though helpful in confirming an identity – is also not enough on its own. Additional factors of authentication enable even greater confidence. For example, a password or PIN code entered in a fashion that the machine recognises as consistent to previous entries will give greater strength to the identity verification.

Biometrics – ie using a physical characteristic to verify identity – are fundamentally nothing new. Fingerprint ID was first developed over a century ago, although it was not digitised. Today the technology is used to unlock iPhones and to gain entry to the Disney resorts in Florida, for example.

The potential for biometrics to solve the authentification problems faced by business are considerable. Though not perfect, they can offer a good customer experience and a variety of different methods are currently being tested and promoted.

Voice recognition, meanwhile, can verify someone in around 15 seconds, quicker than passwords. Yet, questions remain about the accuracy of this method. Can the technology deal with ambient noise? What if the person's voice is impaired due to a cold, for example? Can the technology handle dialects and accents? All of these questions need addressing.

Facial recognition – which is also known as selfie authentication – has recently been incorporated to identify Uber drivers. Again, this method is not without its drawbacks. For one thing, the lighting for the picture needs to be of sufficient quality for it to work. Equally, facial features can change, either by accident or design. Questions still remain about whether the technology can adapt enough to recognise this.

VERIFYING IDENTITY IN THE DIGITAL AGE

Fingerprint recognition is widely used, it's trusted, it's easy, but it is certainly not perfect. Fingerprints can be copied by fraudsters using easily obtained chemicals and the technology doesn't always work first time. Wet fingers, for example, can be harder for devices to scan.

One of the biggest barriers to biometric adoption is trust. With privacy concerns paramount in the digital age, sharing biometric details with outside agencies is not something that individuals would be expected to willingly do. There was interesting news around this recently, however, when a survey showed that far more UK consumers (60 percent) would be willing to trust a bank with their biometric data than the government (33 percent).

It would appear, then, that in the age where convenience is all, consumers are perhaps willing to share biometric details to make their transactions quicker. However, there is still the question as to whether biometrics alone are sufficient to provide robust authentication. There is, for example, the possibility that biometric information could be breached by hackers. Biometric characteristics, by their very nature, cannot be easily changed. What would happen if biometric information was compromised? What is the fall back? It would appear, then, that much like machine learning, biometrics is, on its own, not sufficient.

There is still a crucial role to be played by authentication via manually entered information in the form of a secure password or PIN. Security works at its best when it is multi-factor – a combination of what you have (your device, for example), what you are (a biometric characteristic) and what you know (a password and PIN). This means that the entering of information will continue to have a central role in authentication, either as an addition to emerging identity and verification methods or as a fall back in the event of breach or error.

Passwords, PIN and biometrics all require information to be shared with companies, and consumers need to know that this information will be kept secure. In the wrong hands, personal information can be used to commit fraud and, with the rise in data breaches, fraud is rising too.

In March 2015, Financial Fraud Action UK (FFA UK) published its 2015 year-end report, announcing that: "financial fraud losses across payment cards, remote banking and cheques totalled £755 million in 2015, an increase of 26 percent compared to 2014".

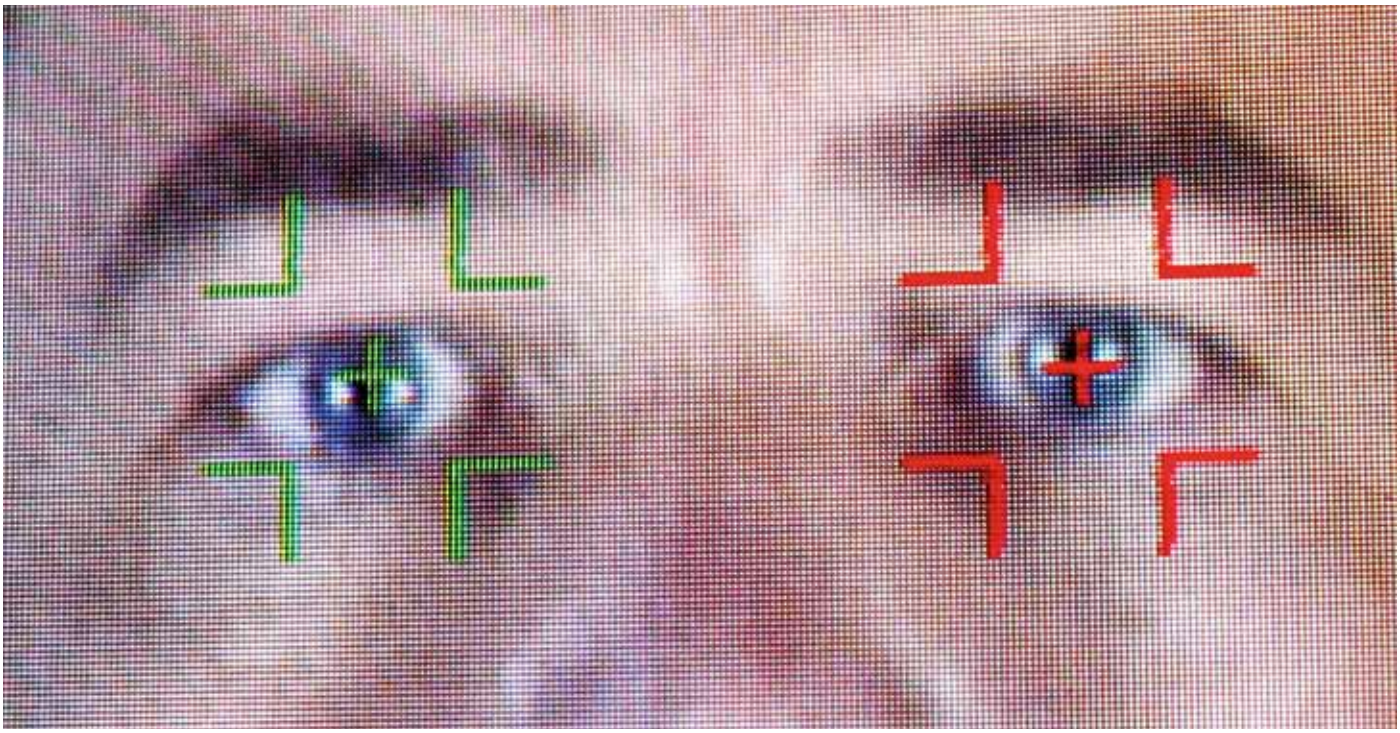
Looking for the causes of this increase, FFA UK was clear about where blame lay: "The rise across all fraud loss types during 2015 owes much to the growth of impersonation and deception scams, as well as sophisticated online attacks such as malware and data breaches".

As already outlined, the dominant form of authentication currently used in digital commerce is the password. Despite its failings, it is still what is most commonly used. Yet as next-generation identity and verification methods, such as biometrics, become mainstream, does this mean that the password or PIN will be obsolete? The answer is no.

Security is at its strongest when there is more than one factor in the mix. Already, for example, iPhone users will be used to unlocking their phones and making purchases through a mixture of PIN and fingerprint recognition. Equally, PIN and password make strong fall backs. As I have previously mentioned, if biometric details fall into the wrong hands, what then? If there is more than one factor at play – if you need both fingerprint and PIN to gain access to financial details – then the biometric details are useless on their own.

The future of identity and verification will not see just one method working on its own, but a number of methods working together to make transactions secure and straightforward. And it is likely that this will be a combination of the new (biometrics) and the familiar (PIN).

David Poole – Head of Growth at MYPINPAD – has 20 years of experience working at the forefront of new technology and payment processes in the UK and USA. He specialises on integration of new payments technology and electronic payments in diverse sectors like hospitality and retail.



Questions still remain about whether facial recognition technology can adapt enough to recognise changes in people's faces