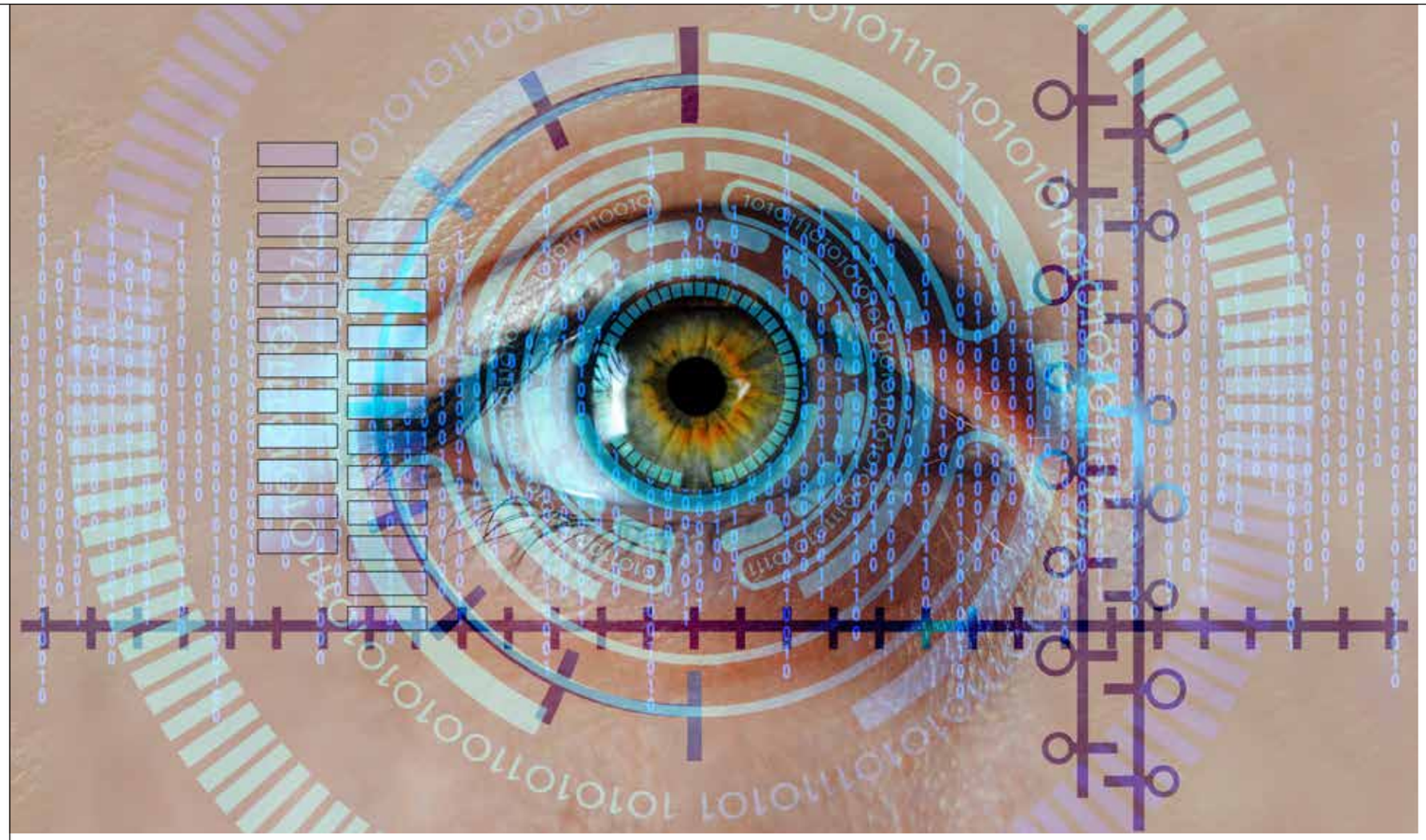

IDENTITY CONFIRMED

Ralf Gladis *explains why biometrics are the step forward for data protection*

It's widely acknowledged that the global pandemic accelerated digitisation, and along with the drive towards contactless payments, consumers have also seen the benefits of adopting biometrics to speed up and ease their payments. But while devices are now being developed to enable fingerprint and face scans or voice recognition, these benefits must be balanced with security. Consumers will embrace new technology and convenient processes, but not if it puts their personal data at risk.

Unlike a password or PIN, biometrics provide a far more reliable form of proof of someone's identity. They take authentication to the next level and this is important against an online backdrop in which faking identities has become a billion-dollar business.

The fact is, security awareness has failed to keep pace with technology or the growth of eCommerce, while storage capacity, processing power and transmission speeds have increased a thousandfold. The average customer is registered with dozens of service providers and retailers, while the main method of customer identity verification – passwords – has remained much the same and can be easily breached by those unafraid of breaking the law.

The pairing of possession and biometrics makes unreliable, often-forgotten passwords a thing of the past

People log in with passwords and secret numbers that are not a serious deterrent for a professional attacker. Primitive codes that can be manually typed in from somewhere do not prove legitimate access at all – only that someone has the necessary knowledge of keystrokes and characters. With cases of keylogging (in which the password is stolen as it is entered into the keyboard), or screen grabbing (in which malware copies the data as it appears on the screen) rising exponentially, more and more customers are at risk of a password breach and the inevitable consequences.

But the problems do not only lie with consumers. Far too many organisations have not strengthened their security posture to match the ingenuity and prevalence of bad actors. They still hold inadequately secured data on their servers making them susceptible to attackers who can gain access to a customer's personal information without breaking a sweat.

To prevent crime around payments processes, the Payment Services Directive (PSD2) introduced Regulatory Technical Standards (RTS) for electronic payments. These standards mean that Strong Customer Authentication (SCA) is required if certain thresholds, such as the number of online orders made in a row, or to a given value, are exceeded.

What constitutes as 'strong'? It's a twofold test – otherwise known as two-factor authentication (2FA). The account holder or credit card holder must identify themselves by means of two of three defined factors. In addition to knowledge (something the user knows such as a PIN or password), what counts are inherence (something the user 'is') and possession (something only the user possesses). Inherence is where biometrics (fingerprint, face, voice, iris recognition or behavioural biometrics such as keystroke dynamics) come into play. Possession usually means proof of having the unique physical object – eg a debit card – in order to make the transaction.

In-store card terminals will allow payment service providers (PSPs) to record biometric verification by fingerprint, facial, eye or voice recognition when a customer pays with an app such as Apple Pay or Google Pay on their smartphone. Looking to the future, Consumer Device Cardholder Verification Method (CDCVM)-enabled terminals will verify whether the consumer presenting the device is the legitimate owner to guard against fraudulent transactions, however these have not replaced standard terminals at the POS everywhere right now.

It is the pairing of possession and biometrics that is particularly exciting, making unreliable, often forgotten passwords a thing of the past. The device determines which biometric method can be used to recognise the person. While Samsung and other manufacturers of Android phones still install fingerprint readers as standard, Apple has now omitted them from its high-end iPhones and is using facial recognition (Face ID) instead. This is what the future will look like.

Biometrics lead to greater consistency and security across transactions – by making inherence the default second factor on and offline. Payment, essentially, should be just another mobile application and in future this will be irrespective of the value being spent.

There is no guarantee that biometric recognition will be a success. The data breaches that make headlines on a regular basis have eroded consumer trust and understandably, they do not want their biometric data used by retailers or any other service provider. The reality is, however, that the data is not used by providers and compliant biometrics are transferred into a 'hash key' from which the original data cannot be extracted or reconstructed. The personal data is kept in a secure element in the smartphone or device where it cannot be tampered with. There is no danger of compromise because it will be automatically compared with the retailer-generated hash key and only processed if they match.

Consumers also like convenience. The ease with which Touch ID, for example, can be used to open a device, or set up a user account, will be a factor in how quickly biometrics are adopted, encouraged by retailers and suppliers whose ideal scenario is to have all their customers registered.

BIOMETRICS PROVIDE A FAR MORE RELIABLE FORM OF PROOF OF IDENTITY THAN A PASSWORD OR PIN

Ultimately, though, how quickly biometrics becomes established as a password substitute depends on whether the pressure from PSD2 allows an ecosystem to grow in which banks, credit card companies, mobile phone manufacturers and network operators pull together with retailers and their payment service providers. Where there are systems, there need to be standards developed collaboratively. Otherwise, initiatives fail to gain traction and they stall.

FIDO (Fast Identity Online), is a standard that specifies how the resources of the end devices – cameras and microphones — may be used for biometric purposes. FIDO is backed by a large international consortium with 250-plus members including not only big names such as Apple, PayPal, Amazon and Alibaba, but also credit card companies and banks (Visa, Mastercard, American Express, Bank of America, ING Group) as well as IT and security companies (Intel, Microsoft, Google, Infineon, Qualcomm, Lenovo, Gemalto, ARM). FIDO-compliant authentication would either be through a separation of the two factors via hardware – if necessary also within a single device – or via software programs that are equally sealed off from each other.

The latest version (FIDO 2.0) even allows a secure connection to an authentication server to be established from the browser. In the consortium's view, this finally makes it unnecessary to check the factors of possession and inherence on separate devices – for example, to confirm an online payment initiated via the PC on the mobile phone.

The FIDO standard is also the key to a more convenient method of biometric identification for consumers. PSD2 allows for delegated SCA. This means that the responsibility for identification can be transferred from the card-issuing bank to the

merchant and de facto to the merchant's PSP. The merchant can optimally embed FIDO-compliant authentication in the purchase process when, for example, logging into the app or the online store. Without delegated SCA, the customer may have to be identified again by the bank when paying, even though they've already identified themselves when logging into the seller. Such double identification is irritating and off-putting. Shifting biometric recognition to the PSP thus removes a stumbling block during check-out, improves security and increases the conversion rate.

THE IDEAL SITUATION FOR RETAILERS IS FOR ALL CUSTOMERS TO REGISTER THEIR BIOMETRICS

Targeted specifically at mobiles, the GSMA (Groupe Speciale Mobile Association), a global alliance of around 800 mobile phone companies, has developed the 'Mobile Connect' system, which identifies customers by their SIM card. Various individual characteristics of the smartphone linked to this mobile phone number can also be used for verification. For data-protection reasons, the customer's consent is, of course, a prerequisite. Mobile Connect uses the OpenID Connect standard, which, in turn, is based on the open protocol OAuth 2.0 (Open Authentication). It provides a possession factor. In the simplest application, the customer receives an SMS on their mobile phone containing a link. If they activate this, they allow the network operator to transmit a customer reference number to the portal operator in encrypted form. The portal operator can then grant the customer access without a password – time and again.

It is not only the issuers of payment cards who are faced with the task of modernising their business processes by means of biometrics. When an everyday routine, such as payment, changes there are ripple effects. The FIDO standard is not limited to use in payment transactions. NFC readers and biometrics could just as easily keep cars, e-bikes and other vehicles secure against theft. They could also mean the end of the key and chip card for hotel guests or tenants of holiday homes, the locker key for the gym, and documentary proof of ID for voters at polling stations. In this way, the banks, notorious for their legacy systems, could even become innovative leaders, pioneering biometrics as they once pioneered IT.

There is an argument that this puts even more emphasis on the importance of smartphones, but maintaining the status quo is the greater danger. A pickpocketed set of keys makes finding a victim's car and stealing it easy, but a mobile phone thief will struggle to do anything with a smartphone secured with biometric authentication ●

Ralf Gladis is CEO of Computop.

The GSMA has developed the 'Mobile Connect' system, which is able to identify customers by their SIM card