# What's the future for biometrics in global payments?

Alex Nasonov

**Alex Nasonov, Worldcore**

**Global payments methods have expanded significantly in recent years, with contactless platforms from tech firms like Apple Pay, Android Pay and Samsung Pay leading the way. But along with these advances in financial services technology, there have been headlines about the mass closure of local bank branches. For example, in the UK over 1,000 high street branches are estimated to have closed in the two years to December 2016[1]. Banking executives are justifiably focusing on both the decreasing numbers of customers using their branches, and the increasing numbers of individuals banking online. Yet despite the increased take-up of technology, the UK's financial services industry remains behind the curve in adopting biometric identification[2]. This article reviews the changes underway and reports on a new survey into how user acceptance – the critical element in the adoption of biometric ID verification – can be maximised.**

The need to increase electronic payment security has clearly become a top priority in the face of growing demand, and the growing threat from fraudsters. According to Financial Fraud Action, in 2016 consumers spent a massive £647bn via payment cards across almost 15bn transactions[3]. Meanwhile, research published last year by consultancy CACI showed that current account customers visited their UK bank branch 427m times in 2015 – less than half the 895m logins on a mobile app[4]. According to UK Finance, the number of branch visits is also forecast to drop to 268m by 2020, while mobile app usage is on track to more than double to 2.3bn[5].

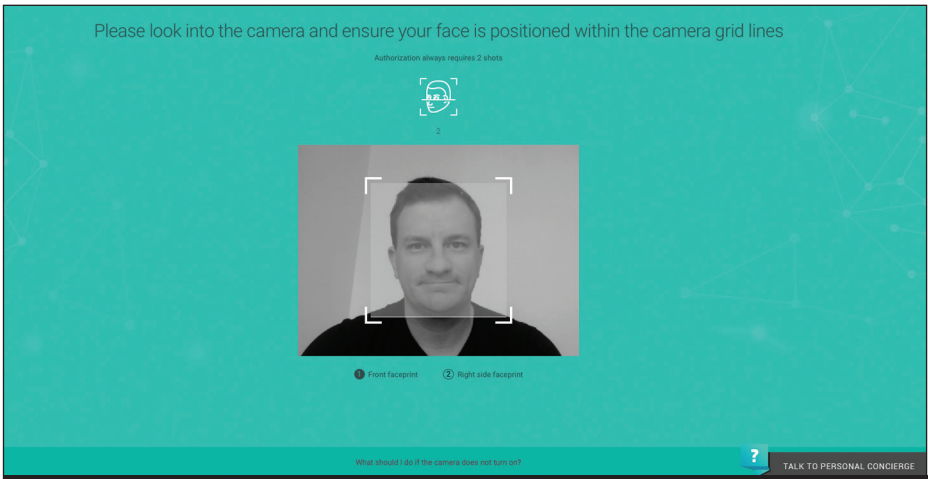
But alongside this tech take-up, financial crime is also on the rise. The Financial Fraud Action report cited above found there were over 1.8m UK cases of fraud relating to payment cards, remote banking and cheques in 2016, involving losses of £768.8m. As the agency says: "During 2016, criminals' use of impersonation and deception scams, as well as online attacks to compromise data, continued to be the primary factor behind fraud losses." Typically, fraudsters purport to be from a legitimate and trusted organisation, such as a bank, the police, a utility company or a government department, and contact a customer through a phone call, text message or email.

In fact chip and PIN, introduced in 2006, represented a major leap forward in card security, but the PIN has innate weaknesses, and the increasing use of contactless payments have raised further security issues. As a result, the enhanced identification verification options available through biometrics are being increasingly deployed by financial services firms to fight identity theft/fraud. The biometric identifiers utilised now include iris recognition, retina, fingerprint, finger geometry, signature, typing, palm prints, palm veins, hand geometry, ear shape, nose, face, odour, voice, gait, DNA and heart (using an electrocardiogram wristband which measures electrical activity from the heart).

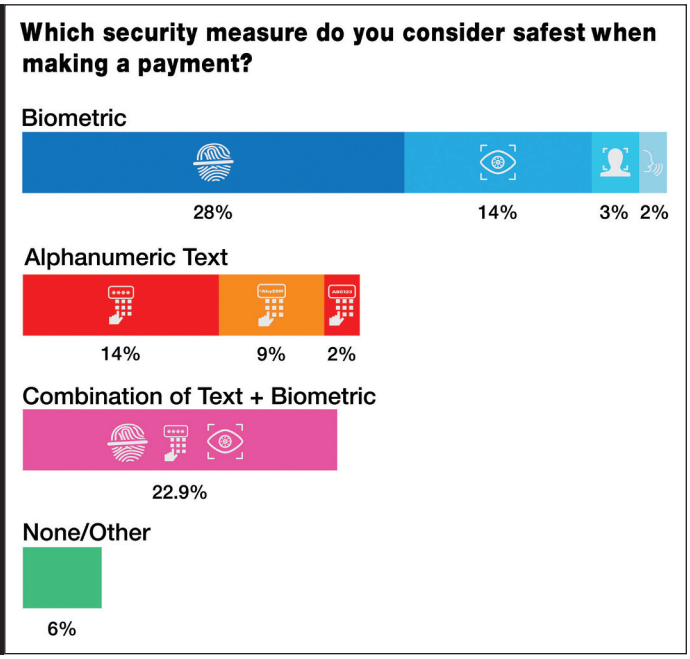
Yet UK financial services firms are lagging behind some world leaders. Last November, for example, an Israeli-based fintech became the first to use behavioural biometrics on mobile devices to replace passwords. The embedded system continuously monitors every in-app activity including the user's finger size, the pressure of the user's touch, and surface touch for financial authentication[6]. Even so, despite the UK financial sector's slow adoption, biometrics are starting to be more widely embraced by banks and card companies:

• In February 2016, HSBC's First Direct subsidiary announced the rollout of voice biometric security technology for telephone banking and for customers using Touch ID on their iOS devices[7]. Its voice biometrics technology works by cross-checking 100 unique identifiers and includes both behavioural features such as speed, cadence, pronunciation, and physical aspects including the shape of the larynx, vocal tract and nasal passages. Customers opting to enrol their 'voice print' are no longer required to recite their telephone security password letters or PIN.

• In April 2017, Mastercard announced that it was rolling out a fingerprint sensor to authorise credit card payments following two successful trials in South Africa with Pick n Pay (a supermarket) and Absa Bank[8]. Cardholders register an encrypted digital template of their fingerprint with their bank or card company. This is stored on the card, and can then be used at any EMV (Europay, Mastercard and




Increasing numbers of financial services firms are turning to biometric technologies, like facial recognition, to beef up their security.




According to Worldcore research, consumers identify some form of biometric security as being the safest when making payments.

Visa) card terminal worldwide by inserting the card into the point-of-sale terminal and placing their finger on the sensor. Mastercard is currently rolling out Identity Check, a new mobile payment app that uses fingerprints and/or facial recognition to verify identity[9].

• During 2016, NatWest trialled a BioCatch biometric system with some business customers to prevent online fraud attempts[10]. The technology captures over 500 points of behaviour, such as hand-eye co-ordination, pressure, hand tremors, navigation and scrolling, to create a unique user profile. Using continuous authentication, it is able to recognise anomalies in behaviours from the point of login and throughout the entire session. The system can distinguish an authorised user's normal human behaviour from that of an unauthorised user, as well as automated BOTs, RATs, malware and other malicious account takeover attacks, where the victim is typically unaware that their banking session has been hacked.

***"The future take-up of biometric ID verification for payments rests on one single core factor – user acceptance... and this remains uncertain"***

• Visa is reported to be testing behavioural biometric technologies to create secure transactions for social payment platforms[11] and challenger banks are also getting in on the act, with the recently launched Atom Bank using face and voice biometrics[12].

However Jonathan Vaux, Visa Europe's executive director of innovation partnerships, emphasises the need for multi-factor identification: "One of the challenges for biometrics is scenarios in which it is the only form of authentication. It could result in a false positive or false negative because, unlike a PIN, which is entered either correctly or incorrectly, biometrics are not a binary measurement but are based on the probability of a match. Biometrics work best when linked to other factors, such as the device, geolocation technologies or with an additional authentication method. That's why we believe that it's important to take a holistic approach that considers a wide range of enabling technologies that contribute to a better end-to-end experience, from provisioning a card to making a purchase to checking your balance."

## Do consumers like biometrics?

Crucially, despite all the technological progress, the future take-up of biometric ID verification for payments rests on one single core factor, user acceptance, and this remains uncertain. Biometric checks help protect both consumers and businesses from fraud, but many individuals are either averse or slow to adopt new technology. Of course, if it's merely a question of making a payment by using your fingerprint, which is significantly easier than remembering and inserting a PIN number, the vast majority of customers should view it as both easy to use and a welcome method of enhancing security. Having said that, payment providers still need to pay considerable attention to educating and familiarising users – a crucial step to embracing change.

To inform this process, Worldcore recently commissioned a survey to gauge consumer views on biometric ID checks. The research first examined which biometric modes are most popular, asking respondents which security measure they felt was the safest to protect them when making a payment. As Figure 1 (*left*) shows, more than a quarter (28%) of those surveyed opted for fingerprints, with nearly the same number favouring 'a combination of traditional password and biometric' security features (22.9%). Perhaps surprisingly iris scanning was chosen by 14% of people, about the same as the top non-biometric security measure – a four-digit PIN code. But as the researchers suspected, many respondents agreed that the use of biometrics provides the safest security method when making a payment (70%). So it would appear that many consumers already accept that biometrics are the future in the payments industry.

Probing further, 60% agreed that using biometric identification will make it harder for someone to hack an account, while 53% noted that an advantage of biometric identification is that it reduces the need to remember lots of passwords. There is, however, a belief among a sizeable minority (42%) that using a mixture of both biometrics and traditional passwords adds an extra layer of security – so there doesn't seem to be an appetite for ditching incumbent CHIP and PIN security just yet. Of some alarm to banks and card companies will be the 7% of people who felt that having to use biometric identification for making payments would be annoying, because 'they couldn't give their password to others to use on their behalf'. Notably, 4% of consumers said that biometrics would make it easier for criminals to steal their identity – conjuring up Hollywood horror stories.

The study then asked people for which types of transactions they would be happy to use 'biometric-only' authentication. Most chose using an ATM to withdraw cash (46%), followed by the 40% who would be happy to use biometrics to validate an in-store payment of up to £30, not dissimilar to the contactless payment threshold. Around 30% accepted the idea of using biometrics to authenticate a standing order or direct debit, but only 28% would use biometric authentication, exclusively, to make an online purchase from a retailer. This statistic seems to belie the increasing number of mobile devices supporting biometric authentication. And people felt less confident about relying on biometrics to make larger payments, such as paying a deposit on a property (11%). The level of challenge still faced by the payments industry is highlighted by the fact that 22% would not consider using biometric identification for any financial transaction – perhaps not dissimilar to early sceptics of the seatbelt?

Clearly, seeing biometrics as the future and actually executing that vision are two distinct things. So the survey sought consumer opinion