Giesecke+Devrient

Trend report

From password to thumbprint

With an ever-changing regulatory landscape, the business opportunity and consumer attitudes towards biometrics are changing.

Technologists have touted biometric identification for years as a safe way to link consumers with services such as mobile payments. Consumers have not been so sure. New European regulations, coupled with ever more accessible technology and a changing financial sector, are changing attitudes and creating the environment for new services and business opportunities.

Consumers are overcoming their reluctance to trust biometrics. Although they've had little direct contact with biometrics until very recently, the idea's been in the public consciousness for more than a century. The forensic use of fingerprints dates from the late 19th century, while Hollywood has made voice ID, facial recognition, fingerprint ID and even internal body scanning biometrics part of its stable of dramatic ideas instantly recognisable by any film fan.

Neither crime nor drama have accurately reflected the potential of biometrics as an exciting or compelling component of the consumer experience. It's perhaps unsurprising that consumer attitudes have been mixed. "Researchers have cited several reasons for reluctance to use biometric authentication technology, including lack of confidence in their reliability (for organizations) and user apprehension", say Rachel German and Suzanne Barber in their University of Texas report, 'Consumer Attitudes About Biometric Authentication'.

They point out that while some 70 per cent of users have experience of and high trust in fingerprint scanning, all other biometric systems attract less comfort. Only 13 per cent of users surveyed had used facial recognition, and only five percent gave it the highest level of trust – 35 per cent giving it the lowest. Across the board, the survey shows that experience of biometrics is essential to build trust, and experience of everything apart from fingerprint scans is still very low. However, that is changing fast – and as the change happens, it is entirely reasonable to expect consumer confidence in different biometric technologies to rise and new business opportunities to become viable as a result. Provided, of course, that the technologies are actually reliable – which they are, as standards bodies recognize.

70%

of users have experience of and high trust in fingerprint scanning

Source: University of Texas report, 'Consumer Attitudes About Biometric Authentication'.

> “Biometric authentication provides customers with unparalleled levels of security but doesn’t require them to jump through hoops to access mobile banking services.”

Jukka Yliuntinen
Head of Digital Solutions at Giesecke+Devrient

These upticks in use are driven by both device makers and regulators. Top tier device makers are keen to differentiate their flagship products, while others – sometimes wisely – wait to see what’s successful before adopting the advances. Although a handful of phones used fingerprint scanners from 2004, it took Apple’s iPhone 5s to make it a must-have in 2013 and a further three or four years to become truly mainstream.

With the technology in place, the regulators are ready. As part of the single European digital market initiative, the second Payment Services Directive (PSD2) is coming into effect in Europe. As with the General Data Protection Regulation (GDPR), this regulatory package is being seen as a template by the rest of the world, especially with its take on authentication. It mandates Strong Customer Authentication requirements (SCA) to protect important or sensitive transactions through multi-factor processes – passwords are no longer enough.

Fortunately for those who have to implement services that fall under PSD2 rules, there’s a set of internationally recognized practical standards that meets that need. Created by the FIDO Alliance – yet another acronym, this time standing for Fast Identity Online – and adopted by the United Nations agency the International Telecommunications Union, these standards are designed to be userfriendly as well as cryptographically secure and compliant with the PSD2 technical requirements.

FIDO’s standards work by having a device authenticate the user locally, and then passing that authentication through a secure channel to the service provider, who decides how to handle the request. That local authentication can be by use of passwords combined with a secure token – some safely generated bit of data that only the user has – or biometrics.

This is more secure than passwords only, and more secure than twofactor authentication that relies on a one-time key sent over text. That can be compromised if an attacker gains access to the user’s telephone number by persuading the mobile operator to transfer it to a new device. In 2016, the NIST (National Institute of Standards & Technology in the United States) concluded SMS two-factor authentication is too risky, and they’re not acceptable under PSD2.

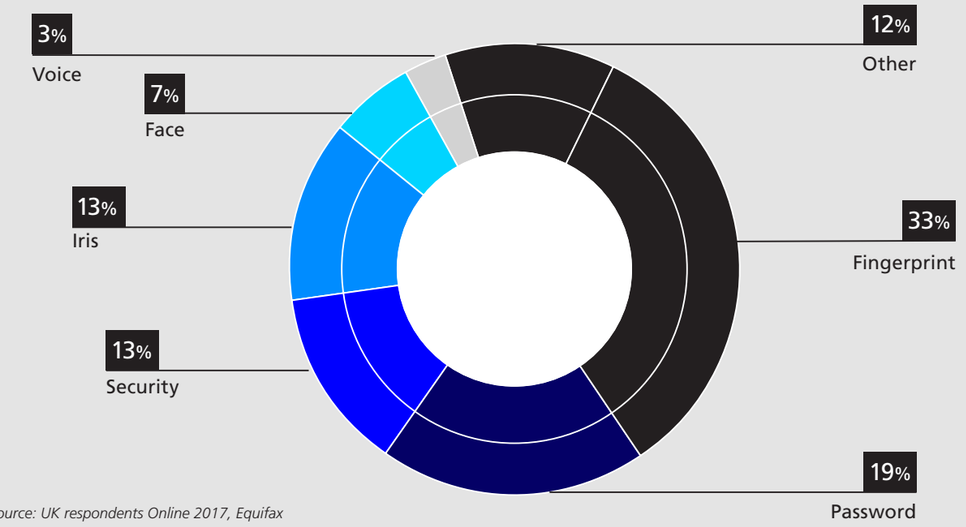
Biometrics, of course, stay attached to their owner.

One of the principle goals of PSD2 is to provide the infrastructure for open banking, where users feel in control of their data and their authentications enough to trust third parties with their financial information. This infrastructure is only newly in place, so first mover advantage is there for the taking in a number of sectors.

In 2017, a survey by Accenture of 2000 UK consumers found that two-thirds did not have that level of trust, with 58 per cent saying they wouldn’t initiate an online transfer with a third party, and a full 82 per cent saying they wouldn’t trust a social media platform with their information.

Going back to the University of Texas survey, 64 per cent thought it somewhat or very likely that strong, effective government standards for safeguarding biometric ID would be introduced. The US lags the EU in adopting such safeguards, but public awareness in Europe is still very low: the combination of

Preferred method to log in to online banking (UK): 56% of Brits prefer biometric banking



Source: UK respondents Online 2017, Equifax

PSD2 and GDPR over time sets the scene for the enhancement of trust in open banking and third party financial services, with no reason to think this won’t eventually equal that felt for classical bricks-and-mortar retail banking and electronic funds transfer via card.

Initial marketing efforts will do well to emphasize the highly regulated and technically secure aspect of the modern remote payment environment – secondary only, of course, to the attractions of the new services it enables.

One example is Giesecke+Devrient’s (G+D) Convego(r) Mobile Authentication. Built on G+D’s FIDO compliant platforms, it uses layered biometrics to authenticate a user prior to a transaction through facial recognition and other factors. Layering improves the quality of biometric recognition, both in positively recognizing legitimate users in different environments and in rejecting attackers trying to impersonate or replicate biometrics.

82%
of consumers say they wouldn’t trust a social media platform with their information
Source: Accenture, 2017

The end result is “much more secure than anything you can do with a PIN card”, according to Jukka Yliuntinen,Head of Digital Solutions at G+D. He says that by moving away from the form-filling and physical presentation of ID that old-style banking needed, a stronger emotional connection with a brand can be formed. “Biometric authentication provides customers with unparalleled levels of security but doesn’t require them to jump through hoops to access mobile banking services”, he notes. “When customers know this, they feel more secure, perform more actions and use more digital services.”

With the advent of 3D cameras in smartphones, as well as in point of sale, the simple act of smiling can be mapped to an animated model of how your face moves – adding much more depth to the data used to confirm who you are.

Biometrics are a big part of making the open banking idea compelling to users, and this opens up a range of new services. “The potential benefits of open banking are substantial: improved customer experience, new revenue streams, and a sustainable service model for traditionally underserved markets” say McKinsey’s Laura Brodsky and Liz Oakes in a report on data sharing and open banking. They identify major disruptions already underway with micro-lending, credit underwriting and peer-to-peer transfers, and cite China’s AliBaba and Tencent as leading the way in integrating payment and finance options with social media and online retail.

Looking ahead, services like Amazon, Apple, Google and eBay all have copious financial and behavioral historical data on their users – data that GDPR makes clear belongs as much to the user as to the services that store them. With the addition of open banking, built on strong authentication, third-party services will be able to offer substantial benefits to users by amalgamating all that information, revealing users’ patterns of purchasing across time and platform and suggesting smarter options – perhaps by forming users with similar requirements into clubs with enhanced purchasing power over suppliers. Instead of selling users to suppliers, the pattern is neatly reversed while user data stays secure.

Such ideas are genuinely new, generating value for both users and service providers within the newly regulated environment that creates the trust that makes innovation possible. Yet appreciation of this new environment has yet to sink in. The field is open to those who move swiftly – for now.

Future Banking – It is all about Securing Payments!

Did you know? Giesecke+Devrient (G+D) technology is unconsciously used by billions of people every day! With more than 700 global Banks putting their trust in G+D and our offerings, we enable secure and convenient transactions for everyday usage.

Founded in 1852 in Leipzig as a printer of bank notes, now with HQ in Munich, G+D is a global powerhouse in payments - be via cash, card or digital services. Our safe payments technology, elegantly combined with smooth customer experiences throughout the whole customer journey, secures the daily life use of financial services. And also creates customer obsession for our clients!

We are: pioneers in payments, industry leader and innovating partner for the financial sector.

Giesecke+Devrient

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

www.mobile-security.gi-de.com/futurebanking
mobilesecurity@gi-de.com

Follow us on: