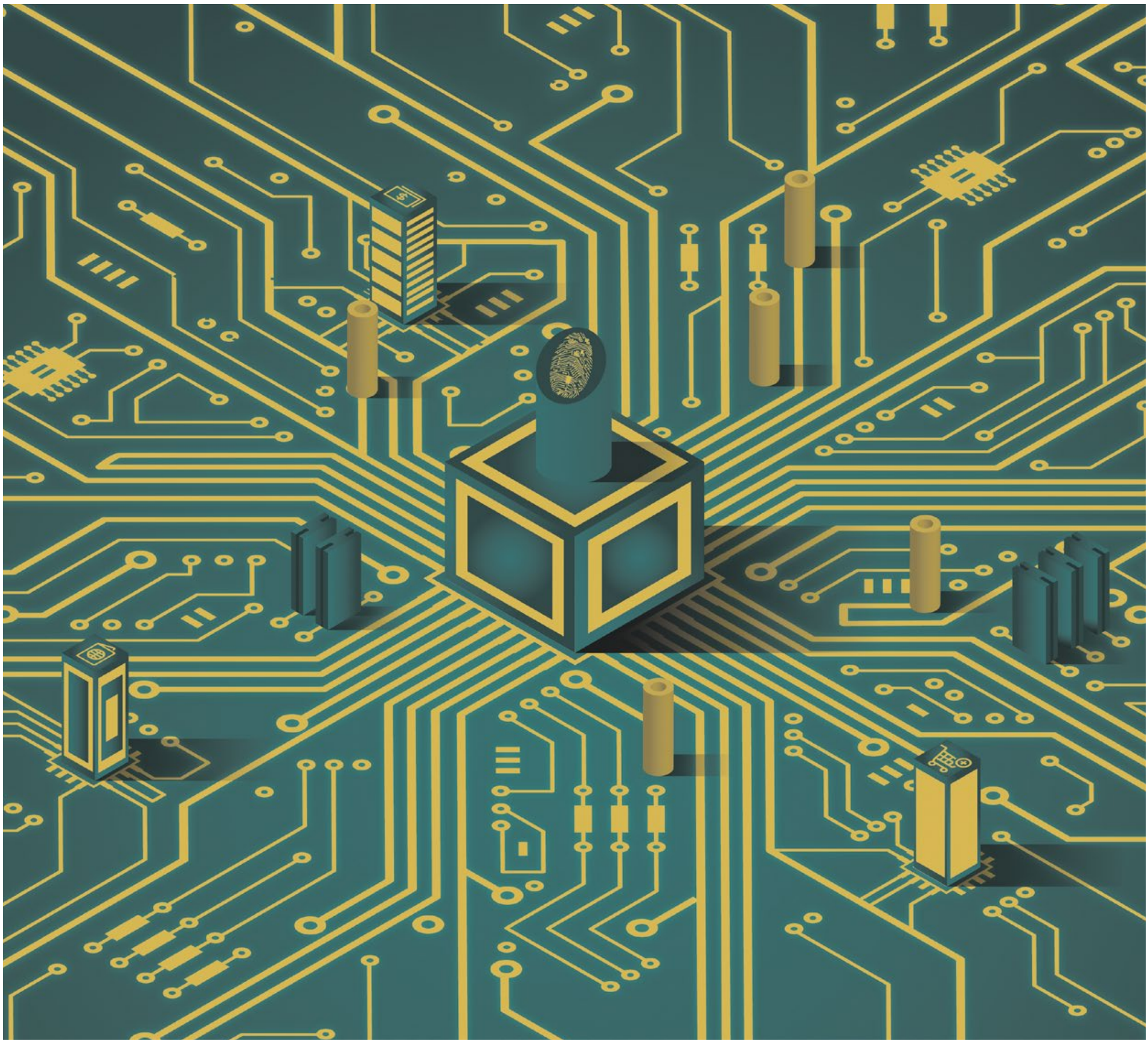
Independent publication by RACONTEUR raconteur.net / # 0313 / 30 / 04 / 2015

BIOMETRICS & IDENTITY MANAGEMENT



Distributed in
THE TIMES

Report partner
Biometrics Institute

Research partner
BIOMETRIC UPDATE.COM

Do biometric technologies spell the end for passwords?

Passwords have been the de facto identity authentication standard for years. But as a string of high-profile data breaches has proven, passwords can be problematic for companies and consumers – is biometrics the answer?

RACONTEUR

Publishing Manager
Nathan Wilson

Managing Editor
Peter Archer

Head of Production
Natalia Rosek

Digital Manager
Jermaine Charvy

Design
Alessandro Caire
Vjay Lad

Cover illustration
Grant Chapman

CONTRIBUTORS

STEPHEN ARMSTRONG
Contributor to *The Sunday Times, Monocle, Wallpaper** and *GQ*, he is also an occasional broadcaster on BBC Radio.

DEREK DU PREEZ
Freelance writer, he specialises in enterprise software and public-sector IT, and contributes to computing publications.

DAN MATTHEWS
Journalist and author of *The New Rules of Business,* he writes for newspapers, magazines and websites on a range of issues.

STEPHEN PRITCHARD
Technology, telecoms and science writer, he contributes to the *Financial Times* and *The Independent on Sunday*.

EMMA WOOLLACOTT
Specialist technology writer, she covers legal and regulatory issues, contributing to *Forbes* and the *New Statesman*.

READ THE REPORT ONLINE

raconteur.net/biometrics-2015

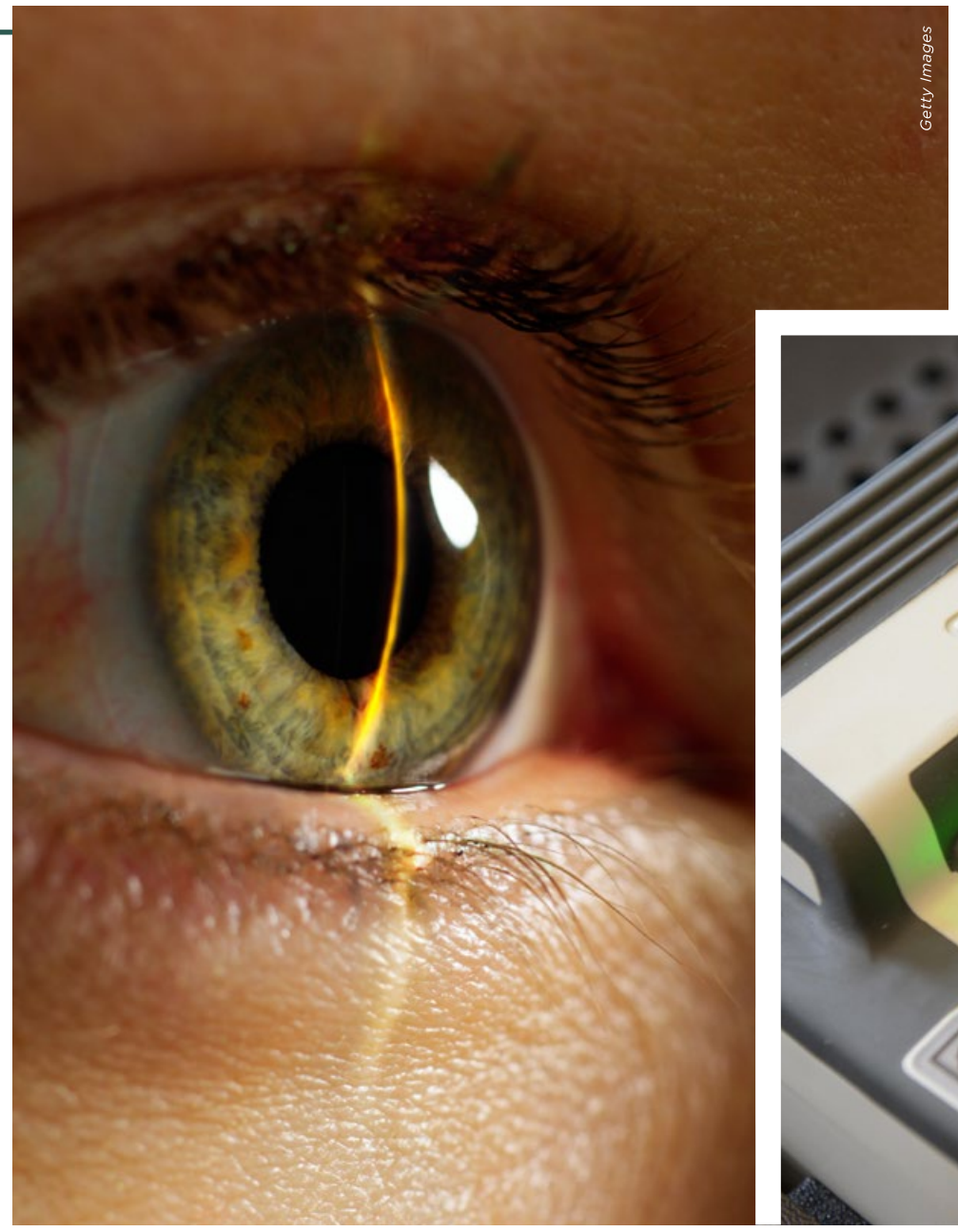
RACONTEUR.net | BUSINESS | CULTURE
FINANCE | HEALTHCARE | LIFESTYLE
STAINABILITY | TECHNOLOGY | INFOGRAPHICS

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3428 5230 or e-mail info@raconteur.net

Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, healthcare, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at raconteur.net
The information contained in this publication has been obtained from sources the Proprietors believe to be correct. However, no legal liability can be accepted for any errors. No part of this publication may be reproduced without the prior consent of the Publisher.

◆ OVERVIEW

● DEREK DU PREEZ


Getty Images

When Apple integrated Touch ID into the iPhone, it soon became clear that fingerprint recognition was not just to make it easier for users to access their smartphones, but was an additional layer of security for new services such as Apple Pay.

While a fingerprint sensor wasn't particularly new technology, its inclusion in the iPhone suddenly meant that millions of consumers worldwide had it in their hands every day and adoption as well as awareness has inevitably begun to grow.

Biometrics suddenly hit the mainstream, and it has since opened up a whole new world of possibilities for consumers and businesses, who can suddenly now buy, sell and transact simply by using their fingerprint and smartphone.

And as Apple Pay begins to take off in the United States, with it widely expected to launch very soon in the UK, many predict there will be an expectation from consumers that they can use biometrics for things other than payments.

"Given that users have now been exposed to the benefits and convenience of this technology on their smartphones, many will want a similar level of convenience in other parts of their daily lives, from using bank ATMs to opening doors, accessing corporate data in enterprise environments or claiming benefits," says Paul Butler, vice president and general manager at identity solution provider HID Global.

"Over time the world of user authentication will continue to evolve and having secure credentials on a smart device will invariably reshape the industry."

And the impact of this is thought to be far reaching. ABI Research believes overall consumer and enterprise spending on biometrics is set grow at an annual compound rate of 29 per cent over the next five years, and that the overall market revenues for biometrics will reach a staggering $26.8 billion by 2020.

Biometrics, of course, extends beyond the Apple ecosystem and companies are experimenting with everything from voice and facial recognition, to monitoring people's heartbeats as a mode of authentication. The implications of this for governments and companies across all sectors is huge, especially given that many have been relying on passwords to identify people for more than a decade.

But passwords have not proven to be entirely effective, given the string of high-profile data breaches from companies such as Tesco, Target and eBay in recent months, which have left customer data exposed.

> **If you can just put your fingerprint on a device, or if you could just show your face or use your voice to authenticate yourself, it's just so much easier from a transaction perspective**

Ajay Bhalla, president of enterprise safety and security at MasterCard, which supports Apple Pay and has a number of other biometric projects live in countries across the world, argues that biometric technology is inherently more secure, given that it is a lot harder for someone to steal your biometric details than it is for them to get hold of your password. This is especially true if two forms of biometric authentication are required to identify somebody or if biometrics is used in conjunction with more traditional approaches to authentication.

"Every day you see incidences where passwords are compromised. Even in my own life, I hate passwords. I probably use 50 applications a day and for each application you're meant to remember a password. It's not humanly possible to remember that many, so by habit you end up using one or two passwords for everything, which leaves a huge risk to systems when they get exposed," says Mr Bhalla.

Measuring eyes, ears, heart and even scent

The number of possible biometric checks on identity is growing as research develops new and sometimes surprising ways of distinguishing particular aspects of physiology

◆ TECHNOLOGY

● STEPHEN ARMSTRONG

Getty Images

It's hard to think of biometric identity technology without picturing Tom Cruise on the run in the movie *Minority Report*. Hunted by killer robots with iris scanning equipment and hailed by animated billboards that use similar tech to personalise their adverts, Cruise is reduced to a full eye transplant to evade capture and death.

It made for a great film, but it didn't do the biometrics industry many favours. Active in one form or another since the invention of fingerprints, the commercial use of biometric data has proceeded in fits and starts over the past 20 years. One possible delay to what was assumed to be inevitable when the movie was released in 2002 is viewers' nervousness about technology that looked creepy and invasive.

"People in the UK have proved wary of eye-scanning systems to date," says Steven Murdoch, principle research fellow in the department of computer science at University College London.

Iris-scanning systems designed to speed up immigration at major airports were scrapped in 2012 after an investment of £4.9 million. Introduced in 2004, the electronic gates and iris scanners were hailed as a "watertight" system for cutting fraud and waiting times. The technology, however, was unreliable and passengers were forced to wait far longer than if they'd simply queued for an immigration officer.

"It may be prompted in part by sci-fi films or may even run a little deeper," Dr Murdoch says. "In Japan, for instance, ATMs use palm scanning technology, which read the unique pattern of veins in the palm of each customer. That's great in a culture that's very concerned about hygiene and would prefer not to touch a machine that other people have used all day long."

While iris-scanning is currently on hold almost everywhere apart from the Mexican city of Leon, which installed scanners for everything from cash machines to paying bus fares back in 2010, other biometric measures are already with us.

Indeed, a recent study by TechSci Research forecast annual growth rates of 14 per cent in the biometrics market, which should reach $21 billion by 2020. "The demand for biometric systems is increasing at a much higher rate in countries such as China, India, Japan and Indonesia when compared with the United States and Canada, due to increasing focus on identity management and curbing security breaches," says TechSci analyst Kalpana Verma. What's changed?

"The greatest advance in biometrics is the iPhone 6," argues Ramesh Kesanupalli, who heads up the FIDO Alliance, an industry-wide lobbying group hoping to establish Bluetooth for biometrics as an industry standard for biometric recognition software.

"Apple's fingerprint recognition is on the home button – the button most users hit many times a day. It's meant biometrics have become about convenience rather than just security, which is speeding up acceptance. It also significantly reduces fraud as applications can send out small challenges to the user anytime and get a confirmation that the phone hasn't been stolen."

Emilio Martinez, chief executive of Madrid-based biometrics company AGNITiO, says: "Biometrics always start with law enforcement. Fingerprints took 100 years to reach the private sector. Now things are speeding up."

AGNITiO's voice biometric technology has been in use by police forces across Europe since its launch in 2004. "When you speak to someone you're listening to their words, to their accent, to the emotion in their voice – our systems do none of that," Mr Martinez explains. "We measure six factors, from larynx to nose to sinuses, which contribute to creating the sound wave that can't be hidden by raising pitch and that's unique to each individual."

The software is now used to identify anything from phone threat callers to your voice when you phone a call centre.

For the future, law enforcements current key target is speeding up a full DNA scan, in theory an impossible test to fake or get wrong. Operating in the field at the moment, the US FBI is testing the RapidHIT 200, which can run a DNA scan in 90 minutes. The Bureau's rapid DNA analysis programme aims to develop "commercial instruments capable of producing a DNA profile to search unsolved crimes while an arrestee is in police custody during the booking process".

> **We measure six factors, from larynx to nose to sinuses, which contribute to creating the sound wave that can't be hidden by raising pitch and that's unique to each individual**

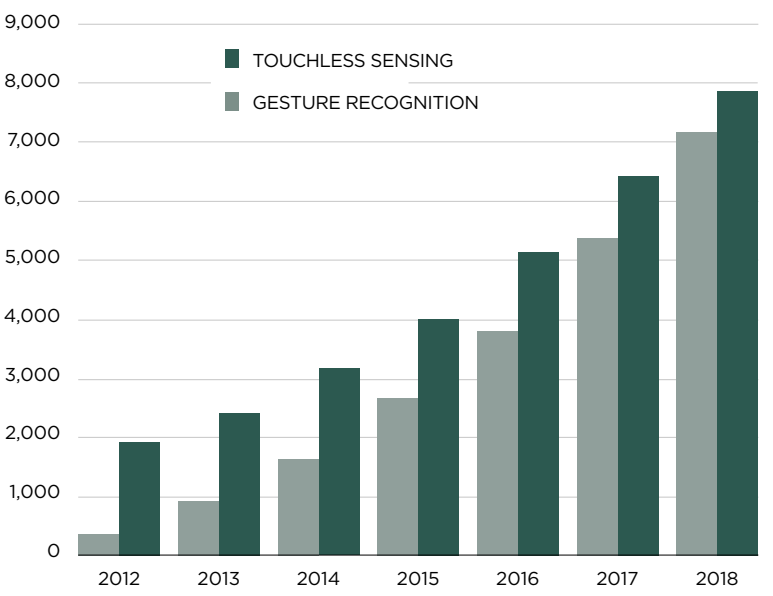
Other systems being trialed include:

- Ear scans – the curved edge around your ears is peculiar to you and researchers in New Delhi are working on an accurate and commercially affordable option
- Heartbeat, breathing and movement – the US Army's STORM has deployed in Afghanistan to identify targets at a distance
- Scent – the US Department of Homeland Security is researching odour signatures to see if individuals have a unique primary smell linked to our genetic coding
- Gait – the US Defense Advanced Research Projects Agency employed gait analysis as a cornerstone of its Total Information system, despite the ease with which gait can be changed by simple factors such as shoes and heavy backpacks.

How long will it take for these systems to reach, say, the financial services industry? "If you're asking about a concerted industry-wide change from something like chip and PIN, then we're looking at years – certainly more than five years," according to UCL's Dr Murdoch. "On the other hand, some banks are already using Apple's fingerprint ID in their apps, so all it takes is one player to switch and that could take as little as a year.

"The main driver for success will be simplicity and ease of use – people just don't want their security checks to get more complicated."

BIOMETRIC SENSORS MARKET FORECAST



Source: MarketsandMarkets 2014

"As well as being more secure, biometrics is of course also more convenient. If you can just put your fingerprint on a device, or if you could just show your face or use your voice to authenticate yourself, it's just so much easier from a transaction perspective."

However, while there is a desire in industry to move beyond the problems of passwords, and consumers appear to be welcoming biometrics because of its ease of use, there are still looming questions regarding who are going to be the leading providers and what biometric technologies will be most popular.

Kevin Dallas, chief product officer of e-commerce at WorldPay, a global payment processing company that works with many of the world's leading retailers and banks, argues that until a common set of standards is agreed, adoption will be tempered.

"One of the main barriers to the widespread availability of biometrics will be the convergence on a standard or a set of standards. At the moment everyone is experimenting, so you see a wide range of approaches," says Mr Dallas.

"We have Apple in particular pushing forward the fingerprint, with the aim of bundling the fingerprint into the iPhone and Apple ecosystem. But will that become the dominate form of biometrics? I don't know. The fragmentation of experimentation is normal in an adoption curve, but it will also slow down the widespread adoption of a set of standards."

Countering the cyber criminals...

The growth in online banking and electronic payments has made it easier for criminals to target banks and their customers – and is prompting the financial services sector to invest in new security measures

◆ **FINANCIAL SERVICES**

● **STEPHEN PRITCHARD**

Banking fraud is a problem as old as banks themselves. Frauds against UK online banking customers netted £60 million in 2014, a 48 per cent increase on losses in 2013, according to Financial Fraud Action UK, an industry body. The organisation warns that individuals are leaving themselves open to fraudsters, by falling victim to phishing e-mails asking for account details or by failing to install effective anti-virus software.

And, with more than half the adult population now using online banking, fraud is likely to grow. Rising losses and the distress caused to customers are prompting banks to look at more robust security measures, including biometrics.

A problem banks face is that online fraud has grown as banking and financial services have become more anonymous and automated.

> **A problem banks face is that online fraud has grown as banking and financial services have become more anonymous and automated**

As one expert in the sector points out, in the days of personal banking and local branches, we had a very effective form of biometric security: a bank manager who recognised their customers. If a bank teller became suspicious of a customer, he or she could call on the manager, who would vouch for the customer or raise the alarm.

Online banking takes away that personal relationship, forcing banks to rely on passwords and other electronic security measures. Unfortunately, passwords are easy to forget and also easy to crack.

"Banks have been overly reliant on PINs and passwords since mainframes first came in, in the 1950s," says Mike Wood, a director at IT firm Unysis. "Banks then moved to PINs and 'memorable' information. Unfortunately that information is often instantly forgettable and people can't recall it when they need to. It is flawed."

To help us remember PINs and passwords, we write them down on sticky notes, store them in spreadsheets or reuse the same passwords over and over. All this makes life harder for the customer, but easier for the fraudster.

Banks' attempts to bolster security, though gadgets such as PIN readers or security dongles, only add to the inconvenience. "These things are complicated, so often we just won't use them," says Mr Wood.

The problem is becoming worse as consumers start using cards and mobile phones for contactless payments on the move. In the UK, contactless payments have no authentication at all if they are less than £20; it is sufficient for someone just to have the credit or debit card.

Phone-based payments could, potentially, support higher-value transactions, but only if security can be addressed. Anything more complicated than entering a standard, four-digit PIN probably will not appeal to consumers trying to pay with a smartphone. Requiring them to enter a strong password – even if they could remember it – might make them abandon the transaction.

This is prompting banks to look for alternative security measures, ideally those that are both hard to hack and easy to use.

Biometrics are, at least on paper, hard to hack, but also convenient to use. Coupled with smartphones with fingerprint readers or computers with webcams, they might not even need banks to give their customers additional hardware.

"Any reliable mechanism that is easier than a password is a good thing," says Dr David Chismon from security consultancy, MWR InfoSecurity.

Already, some banks allow their customers to authorise transactions with a fingerprint and fingerprints are also under consideration as a way to secure smartphone payments.

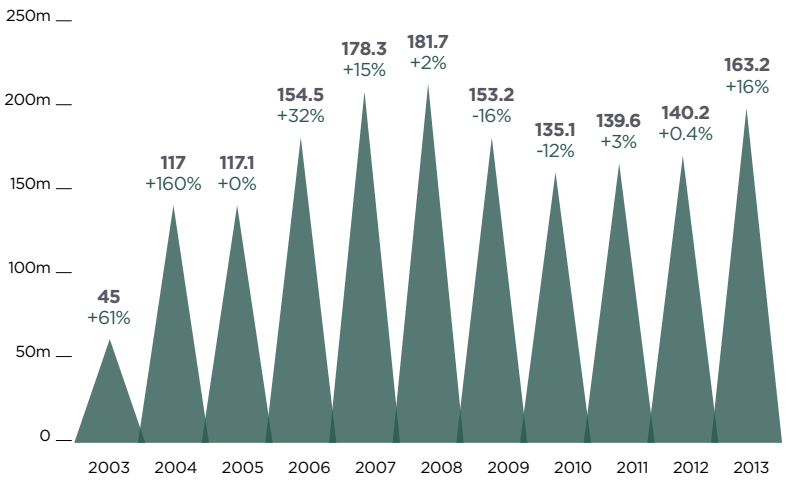
Unfortunately for advocates of biometric security, as well as for banks' anti-fraud departments, biometrics is neither completely secure, completely reliable nor as easy to set up as they might hope. Of the dozens of biometric security trials carried out by banks, only a handful have led to successful, large-scale deployments.

The first challenge banks face is enrolling customers in biometric programmes.

The last few years have seen plenty of new biometric tools join fingerprints and

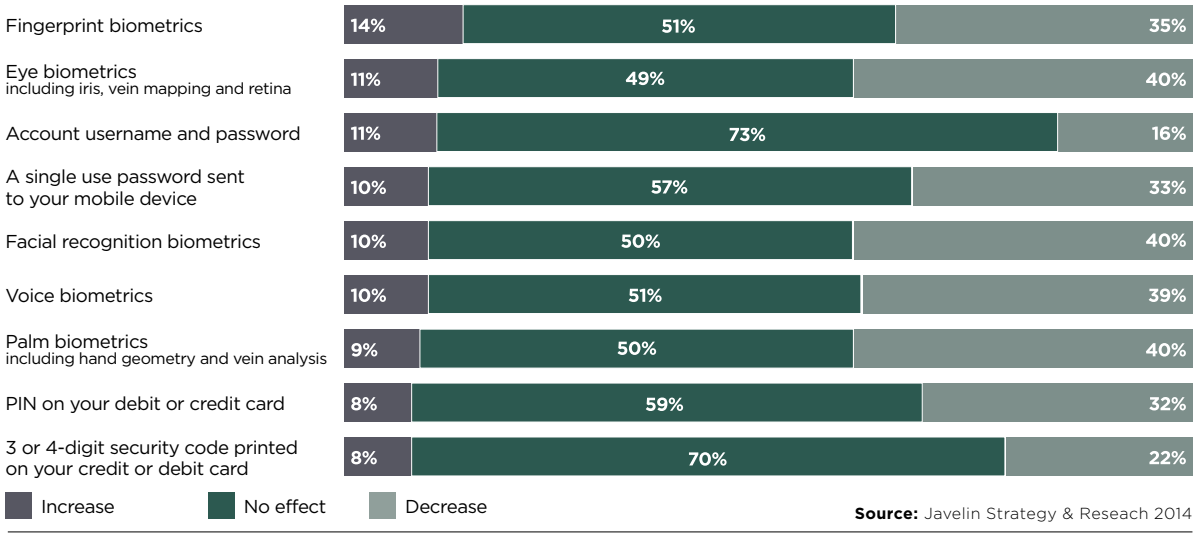
INTERNET/E-COMMERCE FRAUD LOSSES ON UK-ISSUED CARDS 2003-13

FIGURES IN GREEN SHOW % CHANGE ON PREVIOUS YEARS TOTAL (£ EST.)



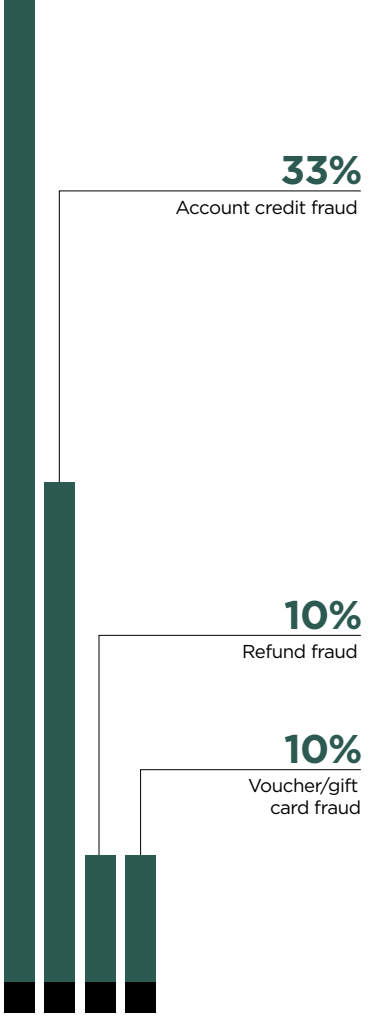
Source: Financial Fraud Action

CONSUMER PROPENSITY TO CHANGE ONLINE PURCHASING BEHAVIOUR DUE TO AUTHENTICATION



Source: Javelin Strategy & Reseach 2014

PROPORTION OF FRAUD INCIDENTS COMMITTED ONLINE



Source: *BRC Retail Crime Survey* 2015

FRAUD FACTFILE

£35.9m losses on remote banking fraud in 2014, up 59% from £22.6m the previous year

£29.3m online banking fraud losses in 2014, up 71% from £17.1m the previous year

£105.5m estimated online fraud against UK retailers in 2013, up 4% on the previous year

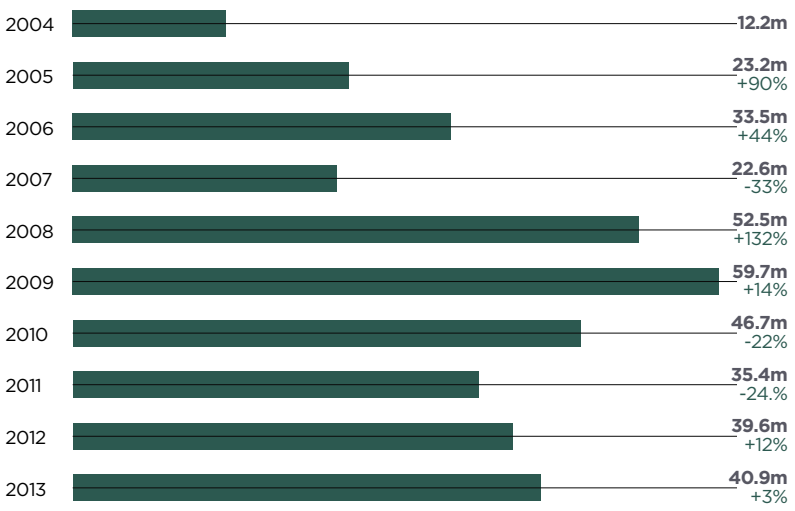
£57.8m estimated UK fraud in 2013 against online retailers based overseas, up 48% on the previous year

Source: Financial Fraud Action

£670m lost to the ten most common online frauds, September 1, 2013 to August 31, 2014

Source: National Fraud Intelligence Bureau

ONLINE BANKING FRAUD LOSSES 2004-13
FIGURES IN GREEN SHOW % CHANGE ON PREVIOUS YEARS TOTAL (£)



Source: Financial Fraud Action

iris recognition. These include advanced voice biometrics, and palm and finger vein readers, systems that read heartbeats, breath sounds, and even the way we write or type, a science known as "behavioural biometrics". As Steve Silberstein, chief technology officer at tech firm SunGard, points out: "The body is full of interesting 'fingerprints'."

But to make these systems work, banks have to capture the customer's biometric ID, as well as check they are who they claim to be. This process is time consuming, expensive and often disliked by customers.

"Enrolment is one of the big challenges. If you have ten million customers, and have to capture their voice prints, that is a significant effort," cautions Steve Nicholls, at consultants Deloitte.

And biometrics, despite the way they are portrayed in science fiction or detective novels, are rarely completely accurate.

Biometrics work on a balance of probabilities or "score". "They don't always work," explains Johnny Wyld, a senior consultant in the financial services practice at PA Consulting. "A password or PIN is either right or wrong. Biometrics produce a percentage score, which the bank has to decide whether to accept – and the customer feels horrible if they are rejected."

> **Biometrics produce a percentage score, which the bank has to decide whether to accept – and the customer feels horrible if they are rejected**

Factors as diverse as background noise to the sweatiness of a palm, can affect a biometrics' accuracy. Banks have to decide whether to accept a lower score – and a higher risk of fraud – or a tougher biometric and the risk of inconveniencing genuine customers, and forcing them back to passwords or memorable words.

"I can't use the fingerprint reader on my iPhone if I've been running," says Tracy Hulver, chief identity strategist at Verizon. "We need a biometric that doesn't have that problem."

It is even possible to fake some biometrics, such as smartphone fingerprint scanners, using little more than sticky tape and glue, warns Candid Wueest, a researcher at security firm Symantec. "That means you can unlock the device, unlock online banking and start a transaction," he says.

This means, at least in the short term, banks look set to use biometrics alongside other checks, such as background checks on transactions, smart cards or phones, and even the humble password. "It has to be seamless, but also allow the customer to keep control," Accenture Technology Labs' Emmanuel Viale concludes.

FEELING THE HEARTBEAT

Halifax, part of the Lloyds Banking Group, became one of the first companies to use customers' heartbeats as a biometric identifier earlier this year.

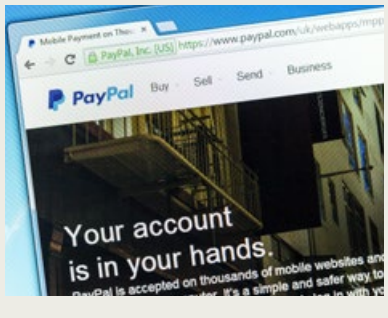
The bank has tested out a device called a Nymi band, to capture heartbeats and use them instead of PINs or passwords.

The Nymi band is similar to wristbands worn by athletes to monitor their heart rate for sports training, but it has been developed specifically to create a heartbeat-based authentication system, which the company calls HeartID. This uses the customer's electrocardiogram, or ECG, which is unique to each of us. The band itself communicates wirelessly with a computer, smartphone or other device.

The system will be used by selected Halifax customers as a way of logging on to online banking on their computers or to authenticate themselves on the bank's smartphone app. It checks both that the customer is wearing the band and the software recognises their heartbeat.

Although the Nymi-band system is being used for online and smartphone banking, it has the potential to be employed more widely, for example to replace PINs at cash machines or even to pay for transactions in shops, provided banks and stores are willing to invest in readers to pick up the band's signal.

POINTING THE FINGER AT RETAIL PAYMENTS



PayPal is one of the best-known names in online payments and is used for thousands of transactions every day, especially on eBay.

But PayPal is also trying to build an offline payments business, for example by supplying card readers to small businesses and retailers. In addition, PayPal customers can use the company's app to pay for goods and services, including meals at the Pizza Express chain.

Last year, though, the company went a step further and added fingerprint approval to its app. The service was set up initially to work with selected Samsung smartphones and tablets because they have built-in fingerprint readers.

The system is designed to replace user names and log-ins, otherwise, anyone wanting to pay by PayPal would have to remember their sometimes complicated computer-based PayPal credentials in a retail store.

The scheme was originally planned for roll out in 25 countries, and was supported by an authentication scheme called FIDO, which was also backed by Google, Microsoft and MasterCard.

However, although other firms have since turned to smartphone fingerprint readers to authorise transactions, including Apple's Apple Pay in the US, security researchers claim the fingerprint system on the Samsung S5 – the launch device for PalPay's scheme – was allegedly easily hacked.

Researchers were able to photograph a fingerprint on a user's phone and create a false print to unlock the handset. However, given the sophisticated tools hackers would need to do this and that they would need to capture the user's fingerprint in the first place, the risks to users could still be minimal.

Biometrics is now being put to

After a relatively slow start, practical applications of biometrics are growing in popularity as take-up in the private and public s

◆ **IMPACT OF BIOMETRICS**

● **DAN MATTHEWS**

The impetus behind biometric technologies is this: who people are is more reliable than what they say or what they hold. People can steal keys, forget passwords and misdiagnose medical symptoms, meaning security, payment platforms and health systems run at sub-optimal levels if they rely on the testimony of human beings.

People can lie, but as yet their physiology cannot. It's why Scotland Yard got so excited more than 100 years ago when it realised fingerprints held the key to locking up criminals and why soon after criminals got so excited when they realised they could wear gloves.

But in the ensuing century biometrics has paved a slow road and only in recent years are its wider applications starting to transition from theory to practical reality. One barrier has been the cost, which is falling, while another is public frostiness, which is thawing.

This area of biotech could be about to take off in a very big way, with thumb-print identification, retinal scans, voice, face and even gait recognition systems becoming ubiquitous in airports, government buildings, schools and hospitals everywhere. But, as of right now, take up is patchy.

In the health sector, for example, biometrics is having a huge impact at the consumer level, with smart gadgets telling people how fast their hearts are beating among other things, but not so well institutionally in hospitals and GP practices, which could be better connected.

> **We have seen the strongest uptake of biometrics in the education sector – it is already successfully in place across a number of schools, colleges and universities in the UK**

For obvious reasons the aviation industry is a front runner in bio-security trials, which if fully successful would prove a thorn in the side of terrorists, smugglers and people accessing countries on false documentation with plans to melt into the populace.

"Airports around the world have successfully completed trials where biometrics enable passengers to traverse the departure process on a fully self-service basis and we have been involved in some of these," says Nick Whitehead, head of strategic services at Atkins.

"We have been involved in the deployment of biometric technology, predominantly using facial recognition. The technology has been implemented for access control purposes, both for managing workers on to and off sites, and securing airport passenger arrivals and departures."

Heathrow and Manchester airports use facial recognition while Gatwick has installed iris scanners; two methods, notes Mr Whitehead, that can be used to solve the same set of problems. And while self-service is not adopted widely in UK airports, it is common in parts of Europe, the Middle East and the Far East.

Though most people passing through these airports don't know it, a central objection to biometric security, the old "big brother" complaint, is being sidestepped. The data captured is single use, wiped clean after the plane lands safely and everyone gets off intact.

Other sectors as diverse as schools and construction sites are dabbling in biometrics, and many technology buyers report that benefits are outweighing the cost for the first time. Yet the potential upside is almost incalculable for organisations big and small.

Take the frankly colossal example of the NHS, currently bursting at the seams because so many people are showing up at accident and emergency departments with problems that could be remedied under non-emergency conditions.

In future, biometric instruments – perhaps bands, implants or home fittings – could tell people the extent of their medical need so health professionals don't have to. It would work the other way too, by convincing hardened war babies that a trip to hospital is not a form of imposition, but a medical requirement.

"There has been considerable global growth in the use of biometrics over the past few years thanks to both government-driven identification programmes as well as increased consumer acceptability driven by access to smartphone technology," says Ajay Bhalla, president of enterprise safety and security at MasterCard.

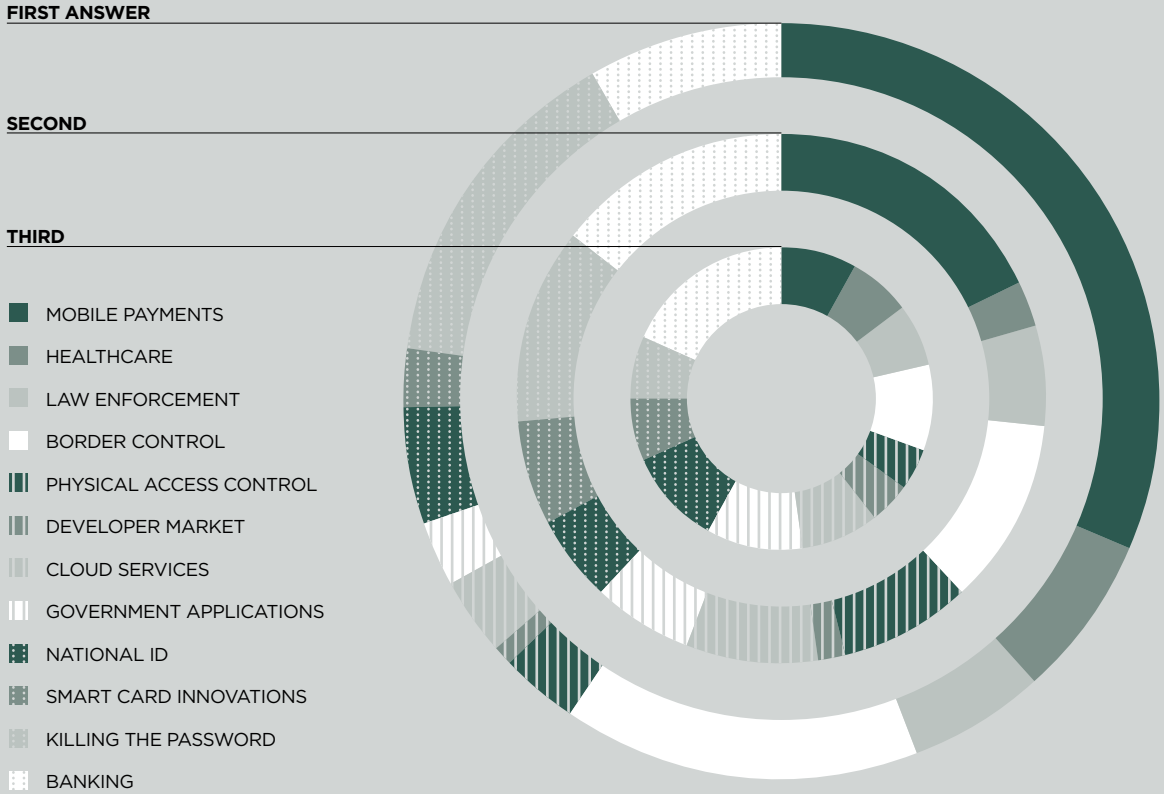
"Looking at Asia-Pacific, it's more and more common to find ATM machines with biometric readers such as thumb-print functionality, so today it's not uncommon to find biometrics in our everyday lives even in forms beyond this," he says.

Dan Bachenheimer, director at Accenture Public Safety, says the roll-out of finger or thumb-print recognition will be hastened because its inclusion in consumer technology is making it more palatable to an initially sceptical audience. On a smartphone, you can opt for fingerprint ID. You try it, you like it; you accept it when the same process stands between you and access to a nursery, hospital, borough council or prison visit.

People who enjoy the convenience of secure point-of-sale technology in their phones will appreciate the same protection when they travel abroad or withdraw cash from a bank. The snowball effect of this should quicken adoption by groups across the whole economy.

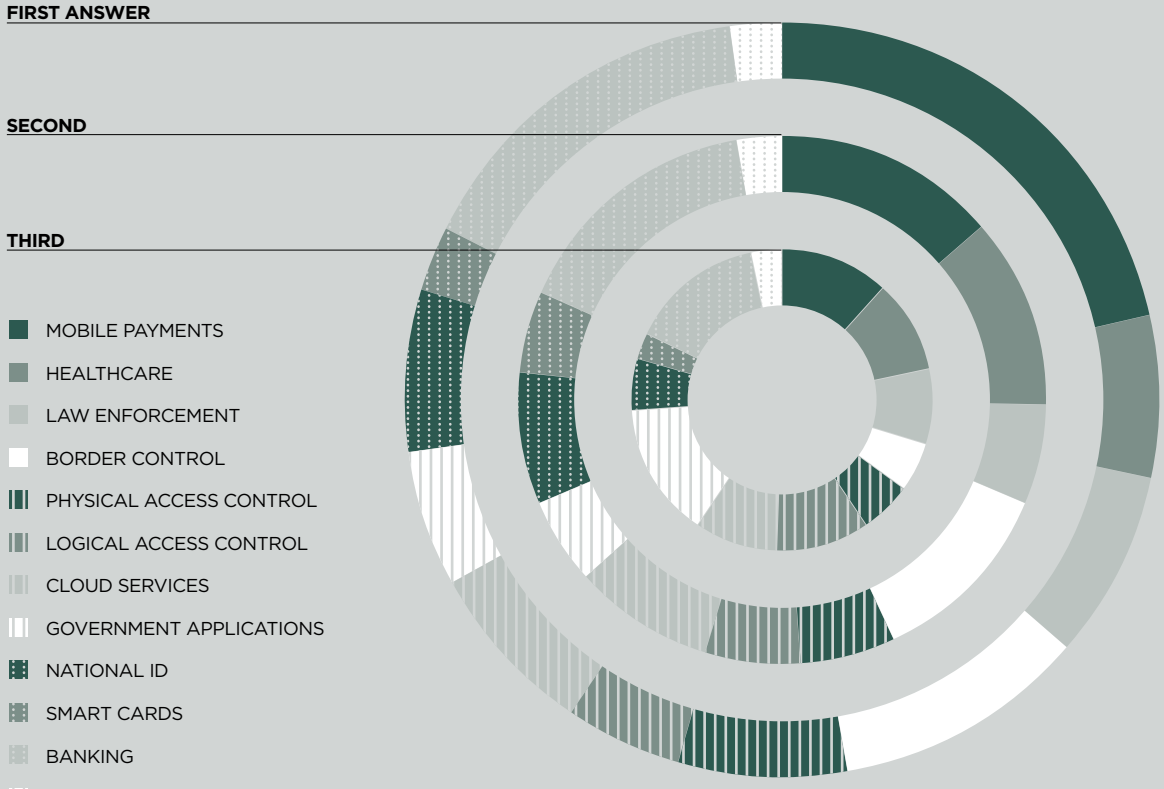
"With advances in biometric technologies and improvements in IT infrastructure, there is a growing acceptance of bi-

WHAT WAS THE HOTTEST SPACE IN BIOMETRICS THIS PAST YEAR?



Source: Findbiometrics 2015

WHICH VERTICAL MARKET ARE YOU MOST EXCITED ABOUT FOR 2015?

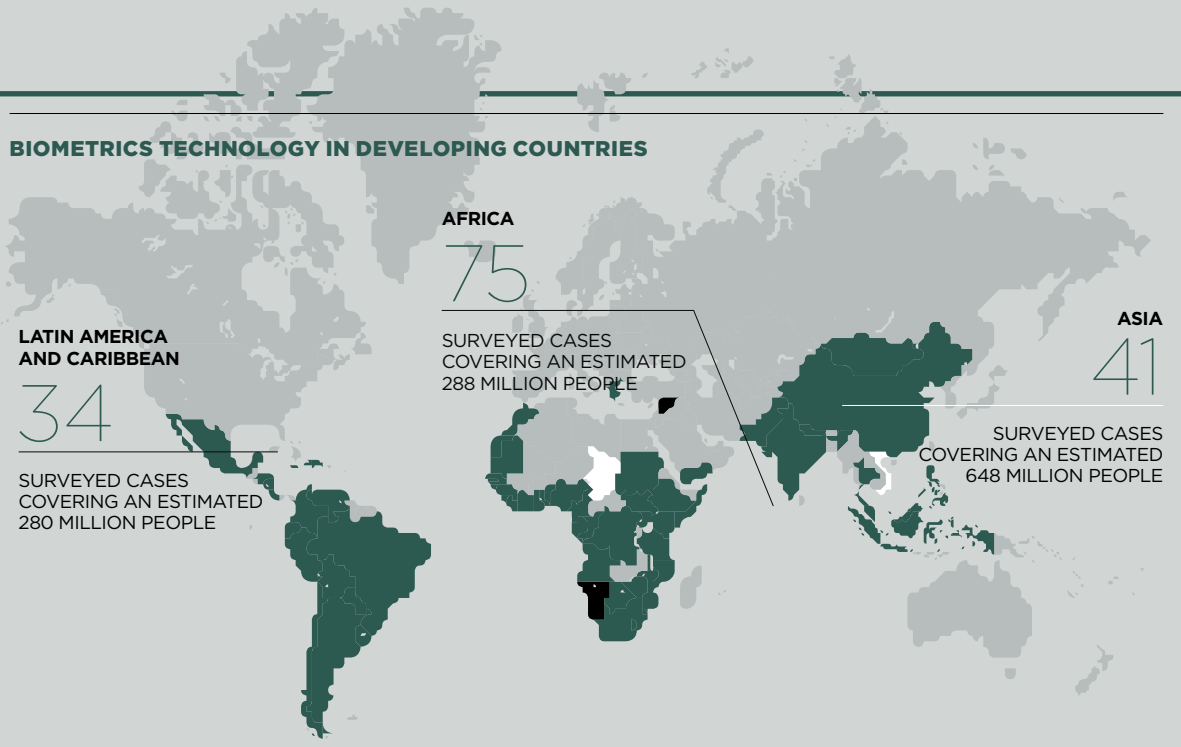


Source: Findbiometrics 2015

work as public fears subside

ectors gathers pace in parts of the UK

BIOMETRICS TECHNOLOGY IN DEVELOPING COUNTRIES



NATIONAL - AT LEAST ONE COUNTRY-WIDE APPLICATION

SUB-NATIONAL - AT LEAST ONE STATE OR MINISTRY-LEVEL APPLICATION

PROJECT - AT LEAST ONE PROJECT-LEVEL APPLICATION

Source: Centre for Global Development 2013

TOP FOUR OF THE MOST PRESSING ISSUES FACING THE BIOMETRICS INDUSTRY

1. **Education - countering misinformation**
2. **The need to ease the integration of biometrics into other systems and applications**
3. **Privacy issues**
4. **Keeping up the pace required to be a player in the developing mobile arena**

Source: FindBiometrics 2015

DEVELOPMENTAL BIOMETRIC CASES BY TYPE AND REGION (NUMBER OF CASES) COUNTRIES

SUB-SAHARAN AFRICA

20 Elections	**8** Financial services
10 Social transfers	**5** Civil service admin
12 Health	**8** Other cases

LATIN AMERICA

9 Elections	**1** Financial services
1 Social transfers	**3** Civil service admin
2 Health	**3** Other cases

SOUTH ASIA

3 Elections	**3** Financial services
8 Social transfers	**3** Civil service admin
3 Health	**18** Other cases

EAST ASIA & PACIFIC

2 Elections	**1** Financial services
3 Social transfers	**1** Civil service admin
1 Health	**2** Other cases

MIDDLE EAST & NORTH AFRICA

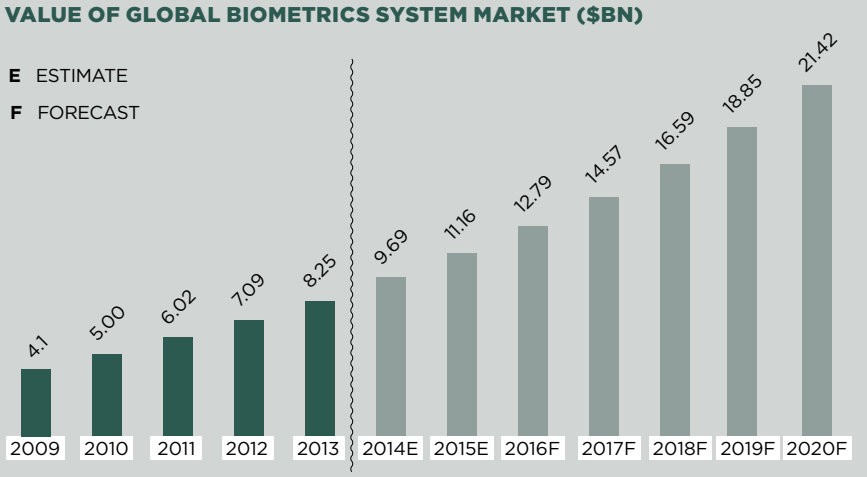
0 Elections	**0** Financial services
1 Social transfers	**2** Civil service admin
1 Health	**0** Other cases

CENTRAL & EASTERN EUROPE

0 Elections	**0** Financial services
0 Social transfers	**0** Civil service admin
0 Health	**0** Other cases

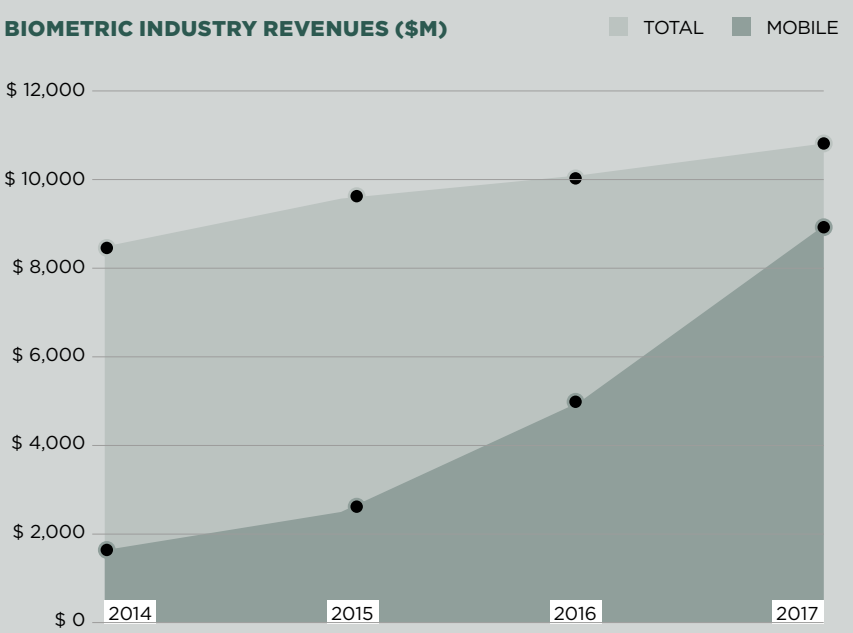
Source: Centre for Global Development 2013

VALUE OF GLOBAL BIOMETRICS SYSTEM MARKET ($BN)



Source: TechSci Research 2015

BIOMETRIC INDUSTRY REVENUES ($M)



Source: Acuity Market Intelligence 2014

ometric recognition technologies in our daily lives, and this acceptance will grow further with time," says Mr Bachenheimer.

"Today, the use of biometric technology on smartphones and other consumer devices has bolstered public acceptance and familiarity with the technology far more than any previous industry deployments combined."

If consumers need warming up, people working in corporate IT are already hot and sold. This is a fertile environment for biometrics. Data security is top of the agenda because most new information companies create is digital, not stored in filing cabinets, but in banks of servers which require several layers of security.

"Biometric technologies are also playing an increasing role in securing company IT systems, providing access to the right people," Mr Bachenheimer adds. "We are seeing biometrics play a growing role in identity and access management solutions, adding the third factor of 'something you are' to 'something you have', such as smart cards, and 'something you know', such as passwords."

For years, the construction industry has been plagued by buddy-punching, where pals clock in and out of work for each other to fraudulently claim pay. Now bosses have the opportunity to eradicate the practice while at the same time improving conditions for workers.

"Biometric technology for workforce management data collection devices can be useful because it identifies and validates an employee's true identity," says Neil Pickering, director at Kronos. "For the employer, this is used to help avoid costly buddy-punching while protecting an employee's personal information.

"It also allows employees to access personal information and self-service features directly from the time clock, including checking their work schedule, verifying their time cards, accessing messages, and even putting in a holiday request."

But it doesn't stop there, technology is also turning up in sectors where you least expect it. "We have seen the strongest uptake of biometrics in the education sector," says Jamie Coombes, at print and IT provider Altodigital. "It is already successfully in place across a number of schools, colleges and universities in the UK.

"It is used in a wide variety of contexts from electronic catering, where students can 'pay' for food and drink using a fingerprint scan, to libraries or within a school's broader IT infrastructure, interlinked with a roaming pull-printing solution."

After years of hype, the technology behind biometrics is finally catching up, giving a real opportunity to upgrade health, financial and security systems across industry. Now the public are taking to the idea too, it 's only a matter of time.

Share this article or infographic on social media **via raconteur.net**

Building the business case for biometrics

Increased business productivity can be achieved through the use of biometric technologies

OPINION COLUMN

RAWLSON O'NEIL KING
Contributing editor
BiometricUpdate.com

Biometrics is defined as both the science and technology of measuring and analysing biological data such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements. Biometrics is the only identification technology that can verify with near absolute certainty the identity of an individual.

Over the past decade, biometric technology has gained wider popularity due to technical optimisation, miniaturisation, software improvements and, most importantly, a fall in price. Reduction in price has allowed a large array of businesses, from small family stores to large manufacturing plants, to adopt biometrics.

Tangible benefits that biometrics offer to businesses of all sizes include time, attendance and workforce management, and enhanced security for healthcare, banking, management and public safety or premise-access applications. Increasingly, biometric technology also speeds financial transactions through point-of-sale systems and third-party processors who leverage biometric-enabled smartphones.

As the technology becomes more understood by businesses, analysts expect to see more deployments by businesses that wish to invest in a technology which enhances security, and increases corporate efficiency and productivity. Consequently, Biometrics Research Group, Inc. projects that the global biometrics market will grow to $15 billion by the end of this year from its 2012 estimated value of $7 billion.

The market for fingerprint biometric technologies will account for the greatest share of the global biometrics market and has continued to be the main source of overall market revenues from 2010 to 2015. This sector was valued at $5 billion in 2012 and is expected to reach nearly $10 billion by the end of 2015.

Face, iris, vein and voice recognition together form the second largest segment. This sector was worth an estimated $2 billion in 2010 and is expected to reach $5 billion in 2015.

> **Growth in the sector can be attributed to increasing popular acceptance of the technology by business in efforts to lower costs, increase output and enhance security**

Growth in the sector can be attributed to increasing popular acceptance of the technology by business in efforts to lower costs, increase output and enhance security. Many companies are now using biometric technologies, such as time and attendance management systems, to improve workforce productivity, efficiency and labour management.

Industry studies have determined that most businesses spend at least 50 per cent of their total budget on payroll and workforce management. Often these processes are manually maintained by staff. High-quality biometric tools, software and equipment, however, can be employed to automate these processes, thereby streamlining labour management in order to lower overall costs and improve bottom-line profitability.

Increasing physical and logical security is also an important use for biometric technology. By using fingerprint scanners, firms can control entry and exit to facilities, thereby protecting infrastructure critical to their operations. This traditional use of biometrics better allows businesses to secure their facilities. The same technology can also be used to guard intellectual property. The use of biometrics to secure computer systems and networks allows firms to protect the operational data which is fast becoming the lifeblood of business.

Typically, businesses have only used passwords or personal information numbers – PINs or passcodes – to protect infrastructure. Studies have shown, however, that passwords and passcodes are insecure and can cost tremendous amounts of money to maintain. Using a singular password or passcode to access such resources makes a user susceptible to security threats because it represents only a single piece of information that a malicious person needs to acquire. Consequently, biometrics can be introduced in addition to existing systems to ensure that they are more secure and to speed access to critical resources.

Biometrics can add a secondary security method for accessing computing and financial resources or physical facilities. Biometrics used in conjunction with more traditional security methods is called two-factor authentication or 2FA. The additional security 2FA provides ensures that additional information is required to sign in to computing resources or access a building.

Two-factor authentication therefore creates an extra level of security which is often referred to as multi-factor authentication. Using a username and password or passcode, together with a piece of information that only the user knows, makes it harder for potential intruders to gain access and steal corporate data, thereby enhancing business security.

Due to the security and financial benefits of biometrics, there is a strong case for all businesses to consider adopting such technologies.

COMMERCIAL FEATURE

FINGERPRINT MARKET SET FOR MASSIVE EXPANSION

When Apple introduced the iPhone with fingerprint identification in 2013, fingerprint sensors went from being an "interesting" technology to a "must-have" overnight. Finally the industry is ready for the massive growth long expected. Among the world-leading players is Norwegian company ***NEXT Biometrics***

Tore Etholm Idsoe
Chief executive

The "Apple effect" cannot be overstated, says NEXT chief executive Tore Etholm-Idsøe. It has made everyone aware of the benefits of fingerprint sensors and, when introduced on iconic Apple products, it caused major players in and outside the smartphone world to follow.

The technology is not without its infancy problems though. The problems relate mainly to size, price and quality. Even in very high volumes, most current sensors are expensive. In order to achieve the price levels necessary to enable integration in smartphones, tablets and notebooks, sensor size is reduced to a level where quality becomes a major problem.

"The true challenge is not about being able to demonstrate if a product works or not, but whether or not you're able to produce a sensor system that works reliably for a high enough percentage of the population every day, and to do so at a competitive price," says Mr Etholm-Idsøe.

"You need to collect the unique features randomly distributed in the human fingerprint and this requires a certain minimum area. The more unique features you capture, the more secure the system is and it becomes less vulnerable to everyday challenges like dirty, cut, worn, dry or wet fingers."

> **At NEXT, we do not have to compromise on size and quality to achieve the necessary price level**

What happens when the sensor area is too small? The number of false rejections sky rocket. Biometric experts around the world have warned of this and now a major university study, the *Madrid Report*, has confirmed this logical connection. To cut sensor size in half leads to at least five times higher occurrence of false rejections. To many this becomes an unacceptable failure rate. Still, in order to stay in the game, the leading industry players make significant compromises on size.

NEXT has patented a different technology than other industry players. The "active thermal principle" uses heat conductance instead of the image collection in the so far dominating capacitive technology. As proven in the Madrid study, both principles work just as reliably, given that the sensor size is the same. However, the NEXT sensor is produced with low-temperature polysilicon display fabs, not with high-cost silicon as is the case with the present market-dominant competitors.

"At NEXT, we do not have to compromise on size and quality to achieve the necessary price level," says Mr Etholm-Idsøe. "Our cost advantage is 70-80 per cent when you compare two sensors of a recommended size and, even when competing with tiny sensors, we still have a cost advantage."

Being able to manufacture reliable sensors at a competitive price has certainly sparked the interest of the market. In November 2014, NEXT Biometrics signed an agreement with a multinational tier-one notebook/ tablet / smartphone company to roll out its fingerprint sensors in multiple products, making it one of only three organisations able to sign such a deal with a world-leading customer.

The start of 2015, meanwhile, saw six organisations place orders for fingerprint sensors to be integrated in small, mass-market products, including payment, home and smartphone-related devices.

"The Apple effect is starting to make a significant impact in multiple new market segments," says Mr Etholm-Idsøe. "The general acceptance of fingerprinting is increasing fast. All of these new customers have made it clear they need the quality of a large-area sensor at a very low price. In this market, NEXT is the only player. These six new projects each represent six-digit volume potential.

"There's significant movement now in what we call 'NEXT-enabled' devices," adds Mr Etholm-Idsøe. "We're seeing a lot of other brand-name players are asking what they can do with this opportunity and how they can integrate them into their devices. There is a surge of interest from manufacturers of devices such as key fobs, home appliances and a range of new and exiting gadgets."

Here, though, reliability is essential and this is where NEXT Biometrics' proven technology creates entirely new markets.

"In a notebook, tablet or smartphone, you have a plan B, so with your present smartphone when your finger is wet it doesn't work, it is an obvious inconvenience, but you can still key in your PIN code," Mr Etholm-Idsøe points out. "In other devices there are no keyboards so people cannot compromise on quality. They need to sell something that will work in 99 per cent-plus of all cases. We are the only player in the world that is able to serve that space."

Unsurprisingly, given the company's unique position in the market, Mr Etholm-Idsøe has big plans for the future and the business is currently expanding to ensure it can keep up with demand. "We sold more than 200,000 units when we started last year and we're now distributing into pilot projects with larger players," he adds. "We're going into millions in 2015. And we are positioned to further multiply our volumes in 2016."

$14.35bn
fingerprint sensor market in 2020
Source: MarketsandMarkets

#3
NEXT is the third supplier to be awarded a contract by one of the multinational tier-one notebook/tablet/smartphone players

150+
companies worldwide presently evaluating integration of NEXT sensors

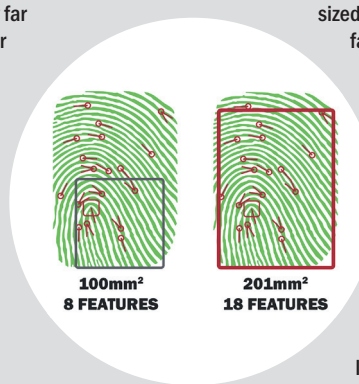
NEXT Biometrics (NEXT:OAX) is a publicly listed company headquartered in Norway, with subsidiaries in Taipei, Shanghai, Seattle, Silicon Valley and Prague

www.nextbiometrics.com

CASE STUDY: MADRID REPORT

Fundamental importance of sensor size proven

A recent study by the Carlos III University of Madrid proves NEXT's competitive advantage. The study is by far the most comprehensive comparative test ever done in the fingerprint industry. Some 80 000 fingerprints were collected from a large and representative group of people, and more than 100 million fingerprint comparisons were made. Sensors from NEXT and two other leading suppliers were included in the tests. World-class hybrid algortithms combining minutie and patterns recognition were used.



The study proved beyond doubt that size is by far the most important factor determining quality in a fingerprint system. If the sensor is too small to capture the full fingerprint image, the quality will drop dramatically. When sensor size is half the necessary area, the number of false rejections will increase fivefold. If the sensor sized is reduced to a third, the average number of false rejections is likely to increase tenfold – to a level not accepted by many users.

The results from the study are in line with what biometric experts around the world have said for years. For NEXT it is a proof of the company's competitive advantage. Today NEXT is the only company able to supply a credible sized sensor at acceptable prices for a mass-market usage. Other suppliers need to cut size and compromise quality in order to reach a price level low enough to be competitive.

The full *Madrid Report* can be ordered through NEXT Biometrics website

◆ **PRIVACY**

● **EMMA WOOLLACOTT**

Protection when tech gets rather personal

Concern over the privacy implications of surrendering personal biometric data may be largely misplaced, but its security is paramount if consumers are to adopt the technology fully

Ask users what they think about biometrics and you'll get a mixed response. On the one hand, many people love the speed and simplicity of the technology as well as, perhaps, its science-fiction image. On the other, however, many have serious fears for their privacy.

Surveys conducted by Imprints, a government-funded research project, indicate that the British public finds biometrics the most controversial and worrying of all means of authentication. Organisations aiming to exploit biometric technology have to be able to show that this, the most personal of all types of information, is safe in their hands.

Privacy fears tend to fall under two headings that hackers could access biometric data to hijack an individual's online identity and personal data provided for one purpose could end up elsewhere.

These fears are in many ways justified. The danger from identity thieves is all the more serious because, unlike a credit card, biometric data can't be cancelled or replaced if it's captured by a third party. And it's constantly exposed, with fingerprints left everywhere and faces on permanent view.

However, contrary to widespread belief, most systems don't store biometric data in the form of an image or recording, instead keeping a mathematical representation of the original characteristic. This representation is then hashed, or transformed by an algorithm, to create the authorisation code.

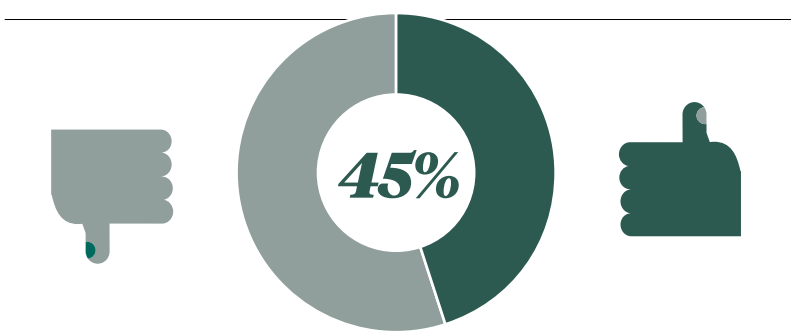
This is the technique used by Nuance Communications, which supplies its FreeSpeech system to Barclays. Customers' voiceprints are now used for authentication over the phone, rather than biographical information such as a mother's maiden name.

> **Most systems don't store biometric data in the form of an image or recording, instead keeping a mathematical representation of the original characteristic**

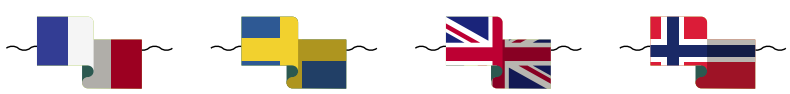
"For the voice biometric to be able to identify you, we create a voiceprint akin to a fingerprint," says Brett Beranek, head of voice biometrics for Nuance.

"But there's a significant difference in that the voiceprint is just an alphanumeric string of numbers that only has meaning to the voice biometrics algorithm. It has no value anywhere other than in that system."

This means, first, that it's not possible to recreate a fingerprint or voice recording from the mathematical representation and, second, if data is ever compromised, new hashed indexes can be issued from the same fingerprint.



of European citizens are in favour of using biometrics to replace PIN numbers for bank cards



52% in favour in France

44% in favour in Sweden

44% in favour in UK

43% in favour in Norway

Source: Steria 2014

"If a hacker got access to the database of voiceprints, there isn't anything they could do with them; they couldn't use them to authenticate anything," says Mr Beranek.

The same applies to Apple's Touch ID, now being used by Royal Bank of Scotland and NatWest customers to log in to mobile banking apps. The system encrypts fingerprint data and protects it with a key only available to the phone's secure enclave.

"The secure enclave is walled off from the rest of the chip and the rest of iOS [mobile operating system]," says Apple. "Therefore, iOS and other apps never access your fingerprint data, it's never stored on Apple servers and it's never backed up to iCloud or anywhere else. Only Touch ID uses it and it can't be used to match against other fingerprint databases."

Other privacy concerns relate to the way data is used and shared. Post Snowden and the leak of classified information from the US National Security Agency, many consumers have fears about function creep, as highlighted by Sir John Adye, a former director of GCHQ, in his evidence to the government Science and Technology Committee.

"What happens to my personal data when I use them on a smartphone for proving my identity? Is Google going to use that data also to target advertising at me?" he asked.

"Is some other commercial company or maybe some hostile foreign government going to use it to target me in some other way? I don't know. We need to find ways of getting that kind of system properly organised."

This, though, is where data protection legislation comes in. "It's personal data, so it needs to be compliant with the Data Protection Act. There should be transparency about what the data will be used for," says Simon Rice, head of group technology at the Information Commissioner's Office (ICO).

"It needs to be stored securely and destroyed when it's no longer necessary so, if a member of a library cancels their membership, say, the library should destroy their fingerprint."

All the same, there's something uniquely personal about biometric data and the government's Science and Technology Committee is currently examining the need for specialised guidelines. It's received a submission from the Biometrics Institute, an impartial group set up by users rather than suppliers to advise on the safe use of biometric technology.

"We want to raise awareness of how biometrics actually works: for the public to understand what it means and that their data is handled in a responsible manner," says the institute's chief executive Isabelle Moeller.

"There are obviously data protection acts around the world with common criteria on how to handle personal information and biometric information should be handled in the same way as biographical information. But we could possibly add other criteria; one could be that the organisation has to conduct a privacy impact assessment."

But perhaps one of the biggest misconceptions about biometric authentification is that it's taking over completely from other security systems.

"Technology can always be hacked – we always say biometrics aren't bullet proof," says Ms Moeller. "They offer much higher security than a PIN and card, but we always take the line that the way forward is with multi-factor authentication."

The ICO's Mr Rice agrees. "We've only got ten fingers so there are only a certain number of possibilities. Passwords or personal questions such as your mother's maiden name allow the individual a bit more control over what data they hand over," he says.

"Responsible organisations will give people a range of options; if people want to use fingerprints, they can, or if they prefer a swipe card they could have that as an alternative. It's something else to add to the mix of security measures – another weapon in the armoury."

PRIVACY POLL

79% of people are concerned about their online privacy

83% of 18-34 year olds are concerned about their personal privacy online

74% would like to have a high level of control over their personal data

68% think UK regulators should have been stricter with Google over breaches of privacy

Source: ComRes 2015

COMMERCIAL FEATURE

IMPROVING SECURITY AND KEEPING TRAVELLERS HAPPY...

Biometric solutions to processing the growing number of international air travellers, ensuring secure identity management and improving customer experience, are at the heart of ***Vision-Box***

The air travel industry is booming. Record passenger demand is pushing airport capacity to the limit. To cope the industry needs a way to process travellers faster, more securely and in a way which improves the entire experience.

The adoption of end-to-end passenger experience and identity management solutions based on self-service procedures and biometric technologies for passenger identification is successfully answering the challenge, and Vision-Box is at the heart of this strategy, with solutions implemented in more than 50 international airports.

With a 20-year experience in the market, Vision-Box is helping airports around the world to improve passenger processing and is already anticipating the future, with the definition of an end-to-end solution that will transform the passenger journey into a sequence of user-centric self-service touch points, from check-in to boarding the aircraft.

A contactless process for the passenger is behind Happy Flow, the pioneering concept which adopts biometrics as the main passenger identification token in an airport, replacing manual control and multiple document verification, such as passport, ID card or boarding pass.

The concept will be implemented at Aruba International Airport, in the Dutch Caribbean, in an initiative gathering relevant stakeholders, and it will reshape the future of identification processes and passenger experience, acting as a reference in airports worldwide in the coming years.

With Vision-Box face-recognition technology, passengers will have their identity assessed at check-in in a self-service kiosk. After that, they will be able to cross every control stage (self-service biometric baggage drop, immigration eGates and self-boarding eGates) quickly and comfortably, simply looking at facial-recognition cameras.

Everyone in the airport ecosystem will benefit – the airport, airline, border control authorities and passengers – while Happy Flow guarantees to eliminate queues, improve security, speed up processing times and ensure holiday makers flow through the terminal with the least possible stress.

> **Happy Flow guarantees to eliminate queues, improve security, speed up processing times and ensure holiday makers flow through the terminal with the least possible stress**

In recent years, Vision-Box's unparalleled experience of deploying automated border control (ABC) solutions has included the largest-ever installation in Europe, involving more than 150 eGates at the UK's largest airports.

Glasgow, Heathrow, Manchester, London Stansted and Edinburgh are some of the airports using Vision-Box eGates to perform the authentication of ePassports and facial recognition in compliance with document and government watch lists. The UK's Border Force is using ePassport gates to process passengers using facial recognition more than any other national border agency in the world.

The lengthy immigration processes in the United States are also being optimised with the adoption of automated passport control solutions. Some 300 kiosks are speeding up processes across some of the main international airports, having in some cases cut waiting times by 70 per cent.

Other examples of Vision-Box airport projects include the world's largest number of multi-biometric ABC eGates at Qatar's new Hamad International Airport in Doha and a nationwide roll-out in Australia of ABC eGates to guarantee accuracy in the identification of passengers before their international departure.

Fulfilling the best outcomes in line with industry standards, Vision-Box works with recognised international organisations, such as Frontex and the International Air Transport Association, to help draw up solutions to integrate with initiatives, including implementation of Smart Borders, Entry and Exit, Registered Traveller Programme, advance passenger information system and pre-clearance, which are underway and will be operational in the near future.

The future implementation of Smart Borders is one of the major improvements foreseen in Europe. Recently, the first out of 14 different European Smart Borders pilots was launched at Lisbon International Airport. Co-ordinated by eu-LISA (European agency for the operational management of large-scale IT systems in the area of freedom, security and justice), the Smart Borders initiative relies on the participation of 12 member states to conduct tests with third-country nationals at specific border-crossing points on a limited set of technical options to validate solutions and concepts.

Vision-Box will contribute by driving the technology assessment at some of these locations, with the implementation of biometric solutions using facial image, fingerprints and iris, but also on the processes using ABC eGates and kiosks to improve security, while facilitating passenger flow. Results of the project will establish some of the foundations for a common, standardised platform to manage the Schengen agreement of 26 European countries that have abolished passport and any other types of control at their common borders.

Vision-Box has developed an integrated global solution to address these challenges: the vb i-shield®, a powerful IT software suite, enables the implementation of an advanced management solution, integrating ABC, security check-point and boarding gates, self-service biometric check-in kiosks and baggage drop units, with advanced digital video management solutions (with intelligent biometric and biographic search engines). This platform enables an overview of the security infrastructure, a person's identity, or his or her stage within the airport journey, as well as flow management, with unlimited scalability.

Additionally, this platform makes possible a cross-match of information and critical data with other platforms of international security organisations, always with data protection in mind, through a privacy-by-design framework.

Outside the airport, Vision-Box has also adopted a holistic approach to identity management, addressing the global challenges of security and people identification: the end-to-end eID Chain of Trust. Starting with a reliable biometric and biographic enrolment of a citizen, the company guarantees a dependable self-service document delivery and an optimised identification in any control point such as a border crossing. On top of all high-quality user-centric interfaces for citizens and operators, a powerful management solution integrates the whole identity chain.

Headquartered in Portugal, Vision-Box has established sales subsidiaries in the UK, Germany, the Netherlands, Brazil, United States, UAE, Hong Kong and Australia. Its solutions now process around 80 million passengers a year.

To learn more visit Vision-Box.com

Biometric Authentication

The critical last foot of security

GoCloudID® the Industry's Only

Cloud-Based • Multi-Biometric • Anonymous-Matching

Identity Verification Solution

IWS® IMAGEWARE® SYSTEMS, INC.

Securing The Future

Visit www.iwsinc.com or contact us at sales@iwsinc.com