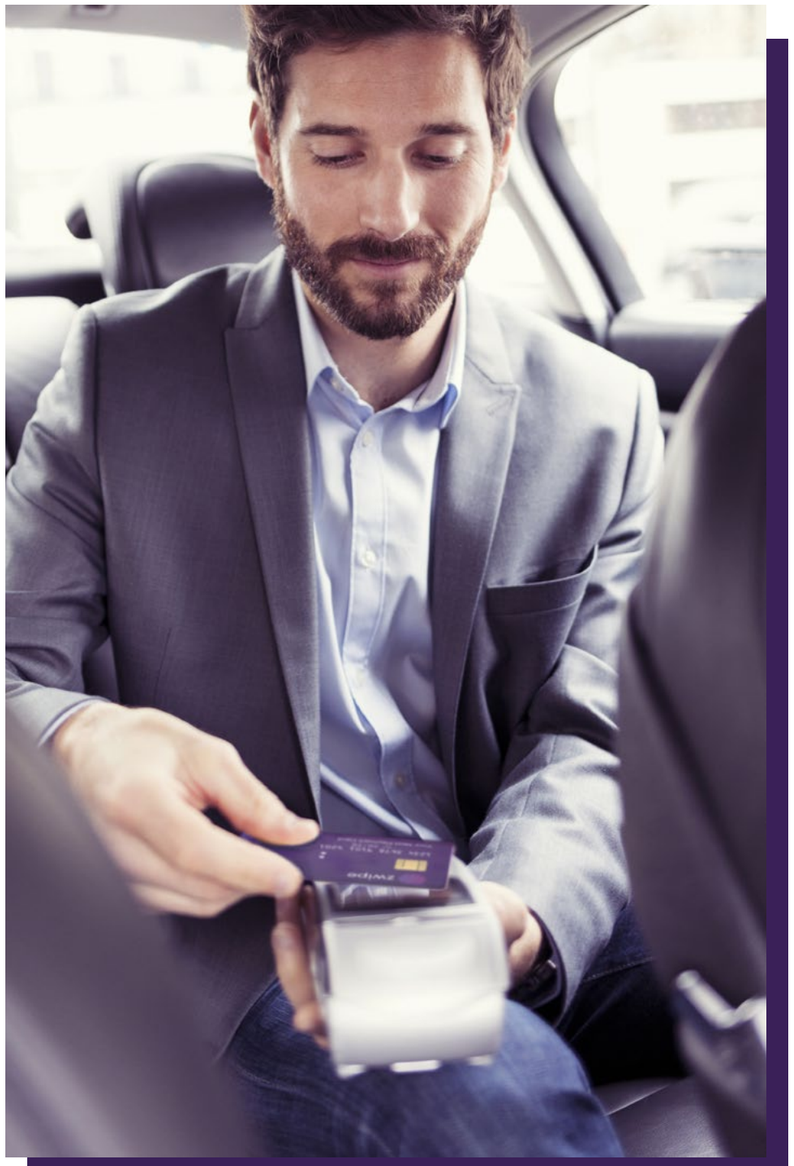
BIOMETRICS DECRYPTED

Great leap forward? Using biometric authentication to win the payment race



THE FUTURE OF PAYMENTS IS HERE AND IT IS YOU

Biometrics in payment is here and it is fast becoming an integral facet of the consumer experience. When given a choice, we consumers, are picking biometrics and the reason why is pretty simple. The speed and ease of use that biometrics enables provides for a much more enhanced checkout experience both digitally and physically.

This report looks to highlight some key developments in biometrics in payments, specifically addressing major industry trends that are driving the entire payments ecosystem to adapt and innovate to meet changing consumer needs and expectations.

On behalf of Zwipe I would like to thank all the leading industry experts who contributed to this report. As a growing technology company we understand the importance of working with strong partners.

Whether you use your fingerprint, your face or some other biometric modality, we believe that the marketplace is ripe for innovation across the entire biometric spectrum. The race to integrate biometrics in payment is heating up across many different segments. The winners will be those who can provide the perfect mix of convenience and security.

Kim Humborstad, Founder and CEO, Zwipe

INTERVIEWEES

1: *Jon Holden,* Head of Security, Atom Bank

2: *Robert Bond,* Partner, Commercial IP, Bristow

3: *Barry Mosteller,* Director Technical Engineering, CPI Card Group

4: *Clive Bourke,* President, EMEA & APAC, Daon

5: *Sylvie Gibert,* SVP Payment Cards, Gemalto

6: *Alan Goode,* Founder, Goode Intelligence

7: *Ichiro Matsuba,* GM, Electronic Components and Materials, Hitachi High-Technologies Corp

8: *Siva Ram,* SM, Information Security and Fraud Risk, HSBC

9: *Sarah Jane Hughes,* Fellow in Commercial Law, Indiana University

10: *Andrew Bud,* CEO and Founder, iProov

11: *James Moar,* Senior Analyst, Juniper Research

12: *Claus Richter,* Head of Cash Management Customer Solutions, Nordea Bank

13: *Travis Tyler,* GM, Consumer Digital, Westpac Group

14: *James Stickland,* CEO, Veridium

15: *Kim Humborstad,* Founder and CEO, Zwipe

TABLE OF CONTENT

Executive summary

ONE STEP CLOSER TO A GREAT LEAP FORWARD

In five years, biometric technology has jumped out of the lab and into the lives of consumers. Apple's launch of Touch ID in 2014 introduced large numbers of technology early-adopters to fingerprint identification, normalising everyday use of biometrics as a safe, convenient way to access devices and solve multiple interlinked problems affecting financial services, including password inflation and cybercrime, and kicked-off a step-change in consumer behaviour in the process.

A much-hoped for biometric wave accelerating the use of biometric identifiers to make payments and complete financial services transactions has been less obvious. While PINs and account passwords increasingly feel like an analogue stop-gap, they have proved, often surprisingly, resistant to disruption as the digital age has gathered pace.

Lessons from the successful introduction and deployment of contactless payments for public transportation and fast-moving retail environments however, have raised awareness of consumer demand for quick, easy payments that don't compromise consumer security – a trend that cuts across all regions. Not to mention the potential to realise much sought-after opportunities to improve the frequency of card use, reduce cart abandonment online, and remove barriers to higher transactions at the check-out.

Incorporating insights from financial services industry experts and the wider biometric technology ecosystem, this research provides a report card on progress toward widespread adoption of biometric authentication for payments and banking including valuable insight on the strategies being applied by innovators and trailblazing institutions to drive merchant acceptance and consumer use.

The last mile of authentication is the final step to unlocking the true potential of the digital payment value chain – as essential to high street retailers as to online merchants. The transition to contactless, and its headline-grabbing success in high profile locations like the London transport network, demonstrate how coordinated collaboration between payment ecosystem players – incorporating an unwieldy combination of public sector providers, technology partners and card-issuing banks - can turn a modest step change into a giant leap forward.

Obstacles remain to a world without PINs or passwords. Biometrically-authenticated payment may still be at a formative stage but, as this research reveals, consumer demand, and significant advances in the understanding of best practice in managing biometrics programmes, mean the opportunity for a game-changing shift is here.

Insights from the research revealed the following key considerations, for organisations considering their own approach to deploying biometric authentication:

Convenience meet security: The virtuous adoption circle

Embedding finger and face scanning tools in smartphones has normalised biometrics for the general population. As users enjoy improved convenience and speed from using fingerprints to open smartphones, increasingly they want those same easy methods from financial service providers.

In contrast, as consumers spend more time online. they are growing weary of 'password inflation', the hassle of multiple logins and PINs, and inconveniences like physical card readers. According to the Norwegian Centre for Information Security, the average person has at least 17 passwords for personal use and 8.5 for work-related accounts[1].

The take-up of contactless cards as proof of consumer demand for convenience is a trend that cuts across all regions, with growing agreement that removing the need to enter a PIN for higher value transactions could remove another point of friction and drive transaction volumes.

A completely frictionless experience may not be the end game however. Insights from interviews reveal that for larger or more significant transactions, customers and business might appreciate and be reassured by some authentication obstacles.

In it together: Ecosystem participants need to work together to drive use and acceptance

While some areas of technological innovation are private-sector led, and eventually regulated and managed by governments, biometrics have emerged from a multi-stakeholder ecosystem. Increased use of biometrics at airports and through digital identification programmes has normalised the technologies and increased public trust in them.

The public sector has driven step changes in consumer behaviour in areas like alternative payment methods - notably, 'contactless' for public transit - which the private sector later leverages. That said, each stakeholder has its own needs. Biometrics raise regulatory questions from governments over data security, and financial institutions worry about handing over security to technology firms, or being 'locked' into device-specific solutions. Collaboration and dialogue between the different stakeholders, including over regulatory questions such as privacy, protection and scope creep, can help all stakeholders find middle ground and appropriate compromises.

[1] passwords12.at.ifi.uio.no/NorSIS/NorSIS_Passwords12.pdf

No one-stop shop: Banks should offer a basket of authentication methods

Providers should offer a range of options, including non-biometric logins. All biometrics have strengths and weaknesses Fingerprints are easy to capture, but they do not work when wet, such as in rainy conditions or if finger-tips are sweaty in hot conditions. Iris and retina scanning can be slow, and may not be effective for those with some eye-related disorders; and voice recognition can be breached, as in the example of twins, and is also inappropriate in noisy conditions or where privacy is lacking, such as open-plan offices. For added security, biometrics should also involve multiple layers: a live biometric capture, a user's device, and stored data, which minimises the ability of fraudsters to hack accounts simply by stealing a device, or accessing biometric data. Some companies are also experimenting with behavioural biometrics which require ongoing information collection about grip or motion, rather than static data like a scan.

Don't let the doom-mongers get you down: The privacy-biometrics debate is heated, but often misguided

Advocates believe biometrics improve privacy by making it harder for fraudsters to hack into a person's account. However, because biometrics can't be changed, critics worry about a 'honeypot' effect. In the unlikely event that a biometric is spoofed or stolen, a person's entire identity is under threat. Precisely because biometrics leverage who you are, rather than what you remember, the risks that accompany their theft are serious. Yet it is important to clarify that biometric technology does not depend on static information capture but on the combination of stored information, a 'live' biometric capture, and the device.

Centralising biometric information can help reduce the risk. Where breaches of personal phone security might go undiscovered, banks which store information centrally can observe and defend attacks. Localising data is the converse approach, meaning the information is not stored on a central 'cloud' which could be hacked. And co-location of biometric information can help overcome the limits of both centralised and localised data storage. Companies can also do more to stress-test their systems, such as hiring 'hacker' firms who can put technologies to the test, and use communications to educate consumers about the steps they take to enhance security.

Chapter 1.
TIME TO STEP UP

Over the last five years, biometrics have expanded rapidly across the consumer space, used for unlocking smartphones, approving ecommerce payments and onboarding new customers. “In the retail or financial space, absolutely everyone is adopting some form of biometrics for protection, whether it’s internal or external,” says Jon Holden, head of security at Atom Bank, a UK challenger bank. The drivers of biometric uptake include growing consumer comfort with them, largely thanks to biometric-embedded smartphones; the frustrations experienced by password inflation in a 24/7 digital age, and the growing sophistication of cyber crime.

Biometrics:
A simple solution in a complex era

Consumer Normalisation	Starting with Apple’s TouchID in 2013 and later widening to banks, e-commerce companies and device manufacturers, consumers are increasingly comfortable with biometrics. Use of mobile wallets such as Apple Pay, Android Pay and Samsung Pay, which allow customers to validate transactions with their fingerprints, is growing and the value of biometrically-enabled mobile payments is anticipated to rise from $600 million in 2016 to nearly $2 billion in 2017[2].
Widening Public Sector Use	Border agencies are among the heaviest users and investors in biometrics, through passports and border control scans. They have also driven other step changes in consumer financial behaviour, like contactless payments in public transit. People’s generally greater trust in the integrity of public technology usages helps drive behavioural changes.
Password Inflation	As people spend more time online, they are having to generate increasing numbers of passwords. Problems worsen if consumers are on the move or overseas, and prompted to re-write passwords they are not accustomed to inserting, as service providers add extra security for unfamiliar logins. And when travelling, people may forget security infrastructures like card-readers. Many want a simplified approach to reduce hassle.
Growing Fraud And Cybercrime	More sophisticated forms of financial crime, from evolving ATM attacks to the rise of mobile malware, are leading financial providers to seek stronger protections. Cybercrime costs the global economy over $400 billion annually[3] and over the next two years, as many as one in four companies is expected to experience a security breach, according to the Ponemon Institute, a research firm.

[2] http://www.techrepublic.com/article/biometric-mobile-payments-will-hit-2b-this-year/
[3] www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf

Security and convenience:
The virtuous circle driving adoption

Until recently the only way to protect bank accounts, passwords and usernames are cybersecurity's weakest link today. By one count, they are the cause of more than three quarters of cyber-attacks[4]. Against this backdrop, many consumers favour a single credential[5], and few options are as all-encompassing, and hard to breach, as a biometric. "By using biometrics, banks have the ability to secure their environment more effectively. Their capacity to reduce fraudulent processing of retail or commercial transactions is incredible," says James Stickland, CEO at Veridium, a leader in strong authentication using biometrics.

"People are generally comfortable in using biometrics without trepidation," agrees Clive Bourke, President of EMEA and APAC for Daon, an identity software company specialising in mobile biometric authentication. "Our experience is that approximately four out of five people will choose to use the biometric option if it is presented to them." Survey data also indicate support. A study by Visa Europe concluded that two thirds of respondents wanted to use biometrics when making payments. Another survey found that almost a third would be more likely to use a bank that offers biometric security[6]. "The market now demands that banks use biometrics for simple access," Mr Stickland argues.

Demand for the technology is strong among young customers, who are more likely to manage their finances by phone: one report found that a quarter of people aged 18-29 would consider changing banks if they weren't offered biometric options to verify their transactions. Atom Bank, has found that older customers, commonly perceived to be less tech-savvy, have also taken up biometric options according to Jon Holden, the company's head of security.

Alan Goode, founder of Goode Intelligence, believes this convenience factor became more pressing in the smartphone era, "If we roll back five or ten years before the iPhone, before mobile technology or apps, there was a decent use of e-commerce in financial services, like online banking and payments. But identifying and authenticating consumers was very much tied to these people using a fixed computer. With the increasing adoption of smartphones and apps, existing authentication technologies - user ID passwords, hardware tokens, and smart cards - are not particularly good".

[4] www.dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/moving-beyond-passwords-cybersecurity.html
[5] www.ponemon.org/local/upload/file/NokNokWP_FINAL_3.pdf
[6] www.intelligentenvironments.com/consumer-demand-banks-adopt-iris-scanning-technology-almost-doubles-two-years/

Why biometrics?

Biometrics are automated systems which identify an individual based on biophysical data unique to that person, ranging from fingerprints, to voice and face, palm veins, and even physical behaviour like grip and motion. Each biometric has advantages and drawbacks (see 'Pathfinder' graphic on page 18-20) but taken together, they herald an improvement on conventional password or PIN-based systems.

- Biometric data is more difficult (although not impossible) to fake or steal.

- Biometrics are convenient – people always have their unique biometric data with them.

- The underlying technologies, from scanners to cameras, have improved and brought down costs, while improving accuracy.

It was the rollout of smartphone-based biometric identification, pioneered by Apple's Touch ID, that set off their current ascent. By 2020, Acuity Market Intelligence predicts that biometrics will come as standard on every one of the 3 billion smartphones sold annually; over 5.5 billion biometric apps will be downloaded every year; and more than 800 billion transactions requiring biometric authentication will be processed on mobile devices annually. This will send revenues for the global mobile biometric market soaring to $34.6 billion in 2020, from $1.6 billion in 2014[7]. Goode Intelligence forecasts that biometric identity and authentication technology, which is compatible with banking applications, will even appear on wearable devices such as watches as early as next year. By its estimates, the market value of biometrics in financial services alone will reach $11 billion by 2020[8].

[7] www.biometricupdate.com/201611/uk-consumer-demand-for-banks-to-adopt-iris-recognition-nearly-doubles-in-two-years
[8] www.findbiometrics.com/goode-biometrics-banking-trends-302036/

A tech timeline, from fingers and faces

Fingerprint and facial recognition technologies have developed quickly over recent years. Apple's installation of Touch ID on iPhones in 2013 "created awareness and drove adoption. People have become comfortable with it," notes James Stickland, CEO of Veridium. The number of biometrically-enabled devices is now growing as Samsung and other Android manufacturers add the technology to their flagship and mid-range models: by the end of this year, one billion smartphones with fingerprint readers will be in use internationally.

Facial recognition has, more recently, come into prominence. Andrew Bud, CEO of iProov, a vendor of facial recognition systems, explains that those systems took a "quantum jump" forward when it became clear that deep learning technology could be applied to faces. "Until 2014, face verification was dominated by a small number of companies who had to make massive investments in order to attain good levels of performance, provided the conditions were controlled. But it didn't work well enough in the rough and tumble of the real world," he says. Now, deep face technology allows users to move around, validate themselves in dim lighting, or even grow a beard or put on glasses without confusing the system. "Suddenly, if you knew what you were doing, you could build systems which performed up to 10 times better than the previous ones and were particularly tolerant of the real world difficulties that had compromised them," he argues.

"What we find is that once people start using biometric technology socially, they become more willing to do so for the more serious stuff like banking, and the hardware manufacturers have already done the adoption and change programme for us"

Travis Tyler, *General Manager of Consumer Digital at Westpac Group, an Australian bank.*

Fingerprint

Advantages	Low-cost and widely available scan technologies, popularised in consumer space by smartphone manufacturers.	Well-understood biometric, after long-standing use by police and security forces.
Disadvantages	Not 100% fraud-proof; fingerprints can be copied using certain materials.	Not always ubiquitous e.g. in cases of skin damage. Fails when finger (or device) is wet, or when finger-tips are sweaty.

The most commonly understood biometric, fingerprints, have long been critical to crime prevention and the justice system, stretching back over a century and in common use through digital databases since the 1980s[9]. Their collection greatly eases the ability of justice and police forces to catch criminals and gather evidence. Every person has a unique fingerprint, as manifested in the shape and form of the ridges and lines at the tip of each finger. Fingerprints are among the easiest to collect, from a technological standpoint. However, they are not entirely tamper-proof; evidence shows they have been copied through the use of putty[10]. It is likely, therefore, that the safest approaches still involve either a second factor like a card, or a further authentication.

Palm

Advantages	Non-invasive and unique, with palm vein patterns set for life even before birth[11]. Veins are hidden under skin, making forgery impossible[12].	Already used in healthcare settings[13]. Non-invasive.
Disadvantages	More expensive equipment solutions, including external scanners.	

A person's palm veins are set for life before they are even born[14]. Palm recognition scanners map the shape and form of a person's palms, gauged from internal veins, and other thermal and tactile features of palm surfaces. Technologies such as those of Fujitsu use near-infrared rays to capture a person's vein pattern which is then verified against a pre-established comparator. Palm recognition also uses light, heat emission and pressure analysis. Asia appears to be the most active adopter of palm technologies.

Voice

Advantages	Ease of use without scan technologies. Through the cloud, it can ensure an attempted fraudster's voice is then known to all parties.	Live (rather than static) biometric, requiring real time participation of the individual.
Disadvantages	Harder for voice biometrics to distinguish twins compared to other biometrics.	People may not be in quiet places, or not wish for others to hear them logging into banking services

A major growth area for biometrics is voice authentication for telephone banking, where traditional security questions are time-consuming, frustrating and easily forgotten. Voice recognition has become popular among banks for authentication, with several rolling out voice ID in recent years. Voices are appealing because the recognition software is non-invasive, remote (i.e. can work over a telephone connection) and low-cost. However, unlike eye based biometrics, voices can be identical - between twins.

Eye scanning

Advantages	Retinas and irises are unusual biometrics in that they are internal to the body, yet observable from outside of it.	Includes 'liveness' detection e.g. that body part has not been extracted.
Disadvantages	Costlier scan technologies. Has been spoofed in some experiments using photographs of eyes laid over a contact lens.	Usage can be undermined by more serious eye disorders.

Iris and retina scanning are two related (but distinct) biometrics that identify an individual based on unique features of their eyes. Retinal scanning identifies unique patterns in a person's retinal blood vessels. Iris recognition examines the structure of the iris, the circular disc around the pupil that controls the entry of light. Both are appealing because they are both 'internal' to the body, yet observable from outside of it. Shortcomings include changes to eyes due to diseases.

Facial recognition

Advantages	Maturing scan technologies and growing usage in smartphone devices	Is not negatively impacted by environmental factors e.g. noise, which can affect voice recognition.
Disadvantages	Privacy concerns, as facial scanning can be done without consent or knowledge.	Accuracy of facial recognition has improved considerably over recent years making it on a par with fingerprint authentication, however it is susceptible to lighting conditions.

Facial recognition systems can identify a person by scanning their facial characteristics and structures. Airports have been among the first adopters of facial recognition, partly because the economics work: a single investment in facial recognition scanners can then process thousands of passengers. Such tools are used in airport security systems from Tokyo and Brisbane to the Netherlands. It is now used in Britain and Wales to spot shoplifters and criminals, and in China, for everything from identifying ride-hailing drivers to controlling access to residential blocks and the making of payments[15]. Ant Financial allows 450 million users to log into online wallets by taking a 'selfie'[16]. Accuracy was not always as high as other biometrics – trials in Japan returned an 18% failure rate and the approach was scrapped in 2012. However, facial recognition technology has greatly improved in accuracy more recently. This has resulted in high profile adoption globally. MasterCard and Visa have both launched payment verification solutions using biometrics including facial recognition, and Apple's iPhone X is also expected to drive use.

[9]www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/
[10]www.ifsecglobal.com/biometric-security-systems-guide-devices-fingerprint-scanners-facial-recognition/
[11]www.cbsnews.com/news/patientsecure-biometric-palm-scan-system-hospital-security/
[12]www.fiserv.com/industries/bank-platforms/multi-platform-solutions/verifast.aspx
[13]www.imprivata.com/why-palm-vein
[14]www.cbsnews.com/news/patientsecure-biometric-palm-scan-system-hospital-security/
[15]www.economist.com/news/leaders/21728617-life-age-facial-recognition-what-machines-can-tell-your-face
[16]www.ft.com/content/ae2ec0ac-4744-11e7-8519-9f94ee97d996
[17]www.findbiometrics.com/fiserv-palm-vein-306156/
[18]www.planetbiometrics.com/article-details/i/5907/desc/korean-bank-to-deploy-palm-vein-recognition/

Finger

- Smartphone login & verification
- Authentication for card-based payments
- ATM authentication for cash withdrawals
- Ecommerce checkout processes
- Peer-to-peer transfers

Voice

- Identification for telephone banking/call centers
- Voice-activated payments
- Smartphone login and verification

Face

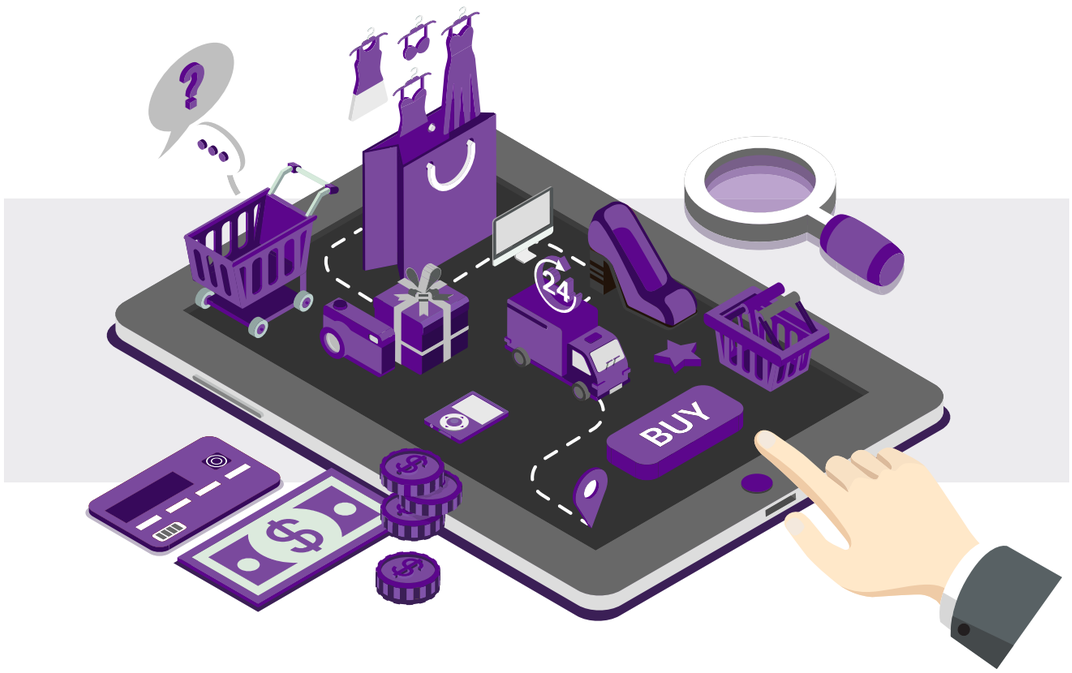
- Validating ecommerce payments
- Smartphone device login and verification
- Approving physical (e.g. fast food, retail) mobile-based payments
- Border security
- Security (shoplifter IDs, authorizing access to residential blocks)

Palm

- Bank branch-based customer authentication[17, 18]
- Physical access control and time and attendance tracking

Eye

- Mobile App authentication/opening
- Verification of larger corporate users
- Accessing confidential data



Chapter 2.
STEP BY STEP

FINGERPRINTS

Fingerprint scanning is currently the most widely deployed and accepted form of biometric identification, regularly used to log into mobile banking apps and transfer money. “This is something consumers want – we now have proof from mobile use that nearly everyone who has a choice chooses fingerprint,” says Kim Humborstad, CEO and founder of Zwipe, a biometric technology company focused on payment cards. “Over one million mobile fingerprint sensors are being manufactured every day and there are billions of transactions using fingerprint to unlock phones on a daily basis.”

Both conventional and disruptor banks are among the adopters. Bank of America, for instance, gave its 48 million customers the option of logging in using their fingerprints in 2015. Today, half of its mobile app users use the function[19]. Westpac rolled out fingerprint verification in 10 weeks in 2014, and found that around half of all its eligible iPhone users adopted the technology virtually overnight. “It was the fastest adoption of any service we’ve offered”, Mr Tyler says. Like many other financial institutions, Westpac still prefers fingerprints to other biometrics. “We have talked to a lot of other banks who offered other options, and the vast majority of take-up is on fingerprint,” he argues. “It comes back to the fact that it’s really simple, and the hardware manufacturers have already done the adoption and change programme for us.”

“The goal of making a biometrics card is to be able to make it a universal card that anybody can use… If you keep the EMV [chip] where it is today, and how it functions today, it’s the path of least resistance,”

Barry Mosteller, *Director, Technical Engineering, at the CPI Card Group, a manufacturer.*

BIOMETRIC CARDS: READY FOR THE MASSES

Biometric credit cards, embedded with a fingerprint sensor which matches a reading against encrypted data stored inside, can help issuers identify theft, prevent fraud and reduce operational costs. Their emergence was prompted by a shift towards contactless payments, says Kim Humborstad CEO of Zwipe which is working with multiple leading card manufacturing partners to bring ‘power harvesting’ cards to market which will with use their contactless interface in place of a battery to take the energy they need from the POS terminal. “Banks and retailers are now invested in contactless because it’s convenient. You can make a stronger case for your card being top of wallet because it’s the easiest way to pay for services,” he explains.

Biometrics can also overcome one of the shortcomings of contactless payments – transaction limits – while maintaining a seamless payment experience for shoppers. “Ideally banks want to make as few changes as possible and fit with consumer habits – so using things like biometric innovation on contactless is a sensible next step by focusing on making it easier to pay with a card,” Mr Humborstad says.

Sylvie Gibert, Senior Vice President Payment Cards at Gemalto points out that, from a consumer perspective most innovations have gone largely unnoticed, with the exception of contactless cards. “Biometrics can change this and banks realise that this is a way by which they can differentiate themselves from their competitors to gain first mover advantage and attract new customers,” says Ms Gibert.

To reach scale however, biometric cards must be compatible with EMV terminals which read chips globally. Several factors have slowed their mass deployment to date. Biometric boards must be adapted to fit within a 0.033 inch card, and cards need to meet international standards requiring flexibility and durability. “Tests require manufacturers to prove that the addition of biometric technology has not undermined the performance of the chip, and they must also meet developing biometric standards. Preparing a card for full certification can take years,” Mr Mosteller said.

Once proof of concept and technology are achieved, pilots ensure that the cards run smoothly. “Not only do they provide an opportunity to test your product, but they help you understand how the consumer will receive the card and what their user-experience will be like,” Mr Mosteller explains. “The process usually starts with “friends-and-family” testing of at least 100 cards, and is followed by a larger, targeted pilot of up to 1,000 cards, involving an issuer,” he says.

Mastercard, which unveiled a biometric card earlier this year following two pilots in South Africa, has come closest to mass deployment. Following additional trials in Europe and Asia Pacific, the company expects a full roll-out of its cards, which aren’t yet enabled for contactless payments, in coming months.
Mr Humborstad, notes that competition in cards rather than mobile payments will drive deployment and adoption. “Idemia and Gemalto have entered the field and are challenging each other, Mastercard and Visa are also taking part – companies are worried they’re losing out,” he says.

VOICE

A second popular banking application is voice recognition technology, which abolishes the need for verification questions in telephone banking. It can also be a useful tool in fraud prevention by capturing the voice of a potential fraudster. “It can weed out bad actors and fraudsters because it there will be a database of voice prints that’ll be associated with people that may be defrauding other banks. That’s the power of the cloud,” says Mr Goode.

Barclays started testing it on wealthy clients in 2013, and after receiving ringing endorsements, rolled it out to all customers last year. To sign up, users have to call a customer service agent to create their own secure “voiceprint” which is made up of over 100 unique characteristics. Over future calls, they can be identified in just a few spoken words, with no requirement for specific words or phrases[20].

Other banks offering voice recognition at call centres are HSBC and Citigroup, the latter of which enrolled 250,000 US credit card customers in voice verification within a year of launching the service in 2015[21]. Last year, Citi became the first bank to roll out this technology in Asia, using uniquely tagged voice prints which cannot be reverse engineered. 35 million of its customers call up agents in the region each year, and voice authentication can cut the time it takes to validate those individuals from 45 seconds to 15 seconds. By March 2017 – less than a year after Citi launched the system in Asia – 1 million users had enrolled[22].

USAA, a lender to members of the US military and their families, uses biometric authentication (including voice) to verify customers through their app even when dealing with customer service representatives. That means that when customers call in, agents already know that the customer is who they claim to be. “It’s short and sweet and it improves the consumer interaction; consumers are very happy with it,” says Mr Bourke at Daon, which provides the technology.

Spanish bank Santander was the first to launch voice-activated payments in the UK although, unlike HSBC and Barclays that also use voice-recognition, they still require customers to enter passwords to open the app itself[23]. This year it launched voice-activated payments for iPhone users in the UK. Once they are authenticated, they can start telling their phone to make payments, move money, or tell them how much they spent. “This pioneering technology has huge potential to become an integral part of the future banking experience,” argues Ed Metzger, the bank’s Head of Technology Innovation[24].

FACE

Facial recognition is an area of growing interest. Atom Bank finds that between its biometric options, face is by far the most popular. “Generally speaking the response to facial recognition has been positive,” iProov’s Mr Bud notes. “The concern about people’s credentials being stolen is different when you deal with a public credential like a face than apparently secret ones like a fingerprint. If you’re dealing with a biometric that they know is public, and you’ve got means to protect them, they feel better about that.”

Mr Bud argues facial biometrics provide “practically the only solution” to stricter anti-money laundering laws and enforcement. “Banks all have to do a strict “know your customer” identity check any time they want to set up an account, and, even worse, go back and check the identities of their legacy customers,” he says. “They had a serious problem there and biometrics, coupled with secure ways of reading documents, present an extremely good solution.”

iProov’s technology, which is used by banks including Norway’s DNB, provides “regulatory-level identity proofing in less than 60 seconds, with the customer sitting in their living room,” Mr Bud says. Users simply download an app, photograph their passport photo page, tap their phone to their passport, giving a reading of their biometric chip, and conduct a face verification. “No more trips to the branch, no more photocopies of documents, no more getting signatures, it is utterly transformative in terms of the customer experience”, he argues.

There range of facial recognition banking and payment systems being launched across the globe includes MasterCard, Visa, Atom Bank UK, Union Bank Philippines (Selfie Banking), Nations Trust Bank Sri Lanka and BNP Paribas (MyBioPass). A significant difference between face and voice biometrics is it allows the service provider, whether they’re a bank or a payment company to retain control of the registration and verification process including user experience, operating thresholds and security which are not as easily accessible with on-device capabilities which are governed by the manufacturer or operating system.

EYE (IRIS AND RETINA)

As hardware matures, some banks are experimenting with younger technologies such as iris scanning. A 2016 survey conducted by Intelligent Environments, a research group, found that 60% of respondents would consider using iris recognition technology, compared to just 33% two years before[25]. Bank of America recently launched a six-month pilot of Samsung’s new technology testing a group of 1,500 Samsung and BofA employees, who were picked to emulate the bank’s customer-base, and aims to gauge whether they find it easy to use, or prefer it to fingerprint scanning[26].

Britain’s Lloyds TSB also launched iris scanning for its mobile banking app in September[27]. TSB believes that iris authentication provides “unparalleled cyber security” because it uses 266 unique characteristics compared with 40 for fingerprints. The bank argues that it is also more user-friendly. “Iris recognition allows you to unlock your TSB mobile app with a simple glance, meaning all of those IDs, passwords and memorable information become a thing of the past,” says Carlos Abarca, TSB’s chief information officer[28].

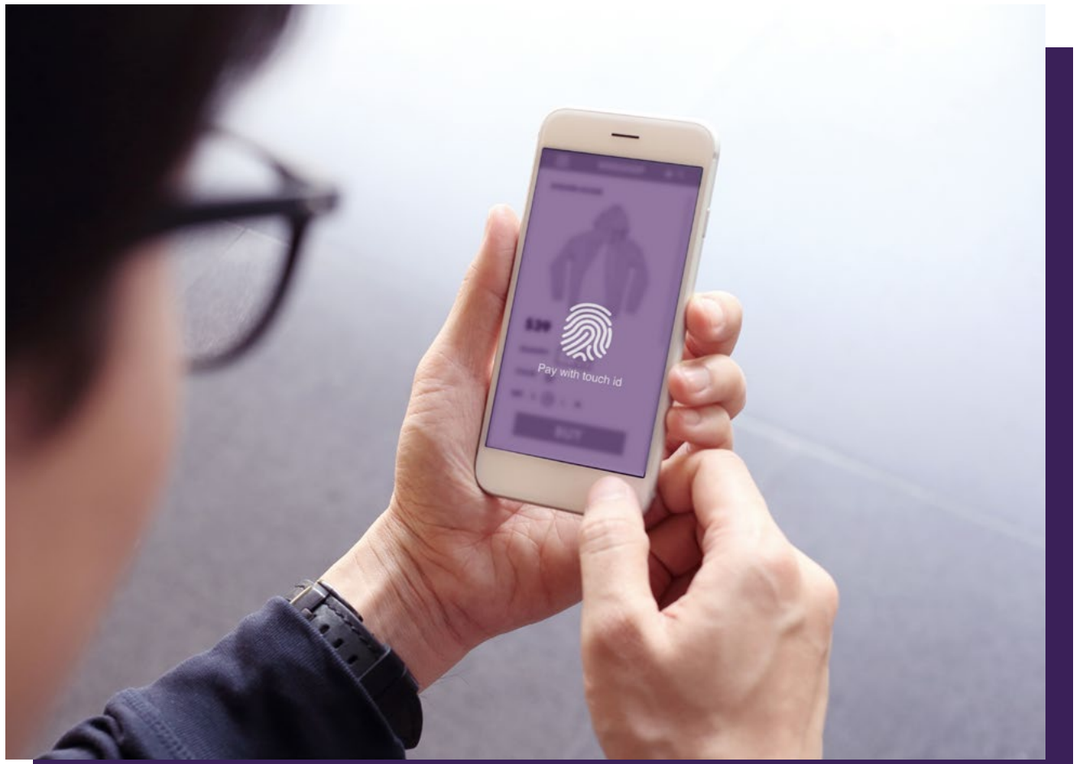
In the US, Wells Fargo has spent more than a year testing a different kind of eye scanner for corporate users who require more stringent security. Its technology comes from EyeVerify, now owned by Ant Financial, which reads unique patterns of eye veins rather than your iris. Unlike finger scanning technology, which sometimes allows several users to validate their identity through a single device, its app recognises only one professional per device, making it safer for large commercial customers to monitor payrolls or complete large transactions. As the system matures, it could replace the physical tokens which financial directors currently use to generate one-time passwords for transactions.

BEHAVIOUR

Some players, including the UK’s NatWest, are now assessing behavioural biometrics, which provide continuous authentication by examining factors like grip, typing movements and other physical behaviour patterns. This makes the technology less suitable for rapid log-ins, but a good addition to security systems which detect malware or unusual behaviour. “I’m a heavy proponent of behavioural biometrics from a background server perspective,” says Siva Ram, Senior Manager, Information Security & Fraud Risk, at HSBC. “This is really about deep learning – payment behaviours, real-time anomaly detection - rather than just the use use of the physical device.”

Among the banks trialling this technology is NatWest, which has applied software from BioCatch to several hundred thousand business customers. It is embedded in the mobile app and online banking site, and creates a unique profile for each user through 500 biometric metrics which range from the angle at which the customer holds their phone to the pressure they exert when typing. By late last year, it had already prevented fraud worth millions of pounds.

[19] www.newsroom.bankofamerica.com/press-releases/consumer-banking/bank-america-introduces-fingerprint-and-touch-id-sign-its-mobile-ban
[20] www.wealth.barclays.com/en_gb/home/international-banking/insight-research/manage-your-money/banking-on-the-power-of-speech.html
[21] www.maparesearch.com/growing-demand-for-biometric-security-in-banking/
[22] www.citigroup.com/citi/news/2017/170321b.htm
[23] www.theguardian.com/money/2017/feb/18/santander-voice-recognition-banking-ditch-passwords-send-money-speaking
[24] www.santander.co.uk/uk/infodetail?p_p_id=W000_hidden_WAR_W000_hiddenportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_pos=1&p_p_col_count=3&_W000_hidden_WAR_W000_hiddenportlet_javax.portlet.action=hiddenAction&_W000_hidden_WAR_W000_hiddenportlet_base.portlet.view=ILBDInitialView&_W000_hidden_WAR_W000_hiddenportlet_cid=1324582960727&_W000_hidden_WAR_W000_hiddenportlet_tipo=SANContent
[25] www.intelligentenvironments.com/consumer-demand-banks-adopt-iris-scanning-technology-almost-doubles-two-years/
[26] www.americanbanker.com/news/the-eyes-have-it-bank-of-america-samsung-pilot-iris-scan-logins
[27] www.tsb.co.uk/news-releases/tsb-customers-first-in-europe-to-benefit-from-secure-simple-iris-recognition/
[28] www.tsb.co.uk/news-releases/tsb-customers-first-in-europe-to-benefit-from-secure-simple-iris-recognition/



Accelerating digital payments

While banks and conventional financial service providers are looking into biometrics, ecommerce platforms and financial apps are also using them to authenticate and approve payments. Growth in social payments and ecommerce platforms is also deepening the penetration of biometrics into finance.

PayPal, through its OneTouch system, enabled biometrics for mobile users on the Android and Apple mobile systems[29], letting consumers check out without having to type in usernames, passwords or billing information, across participating merchants. In China, Alibaba launched facial recognition technology with Alipay, the mobile payments service, back in 2015; the app validates mobile payments by matching a photo at the time and place of purchase, with a stored archive. In September 2017, Ant Financial, part of Alibaba, launched 'smile to pay' facial recognition service in a trial with fast food chain KFC in Hangzhou province[30]. Amazon has also sought patents for its own facial recognition tools[31]. Peer-to-peer money transfers are another growing segment enabling biometrics to smooth the user experience. Venmo, part of PayPal, launched Touch-ID security authentication in November 2014[32]. Its rival, Square Cash, followed suit in January of the following year. There are also national-level biometric identification programmes, the most famous of which is India's Aadhaar, an electronic identification scheme which includes 1 billion people. The programme, which channels welfare payments amounting to $40bn per year, had long suffered from 'leakage' as money did not reach beneficiaries. Start-ups are also exploring ways of combining blockchain and biometrics to enable a person to manage all their financial activities on their mobile[33]. Humaniq aims to bring financial services to the world's two billion unbanked customers using biometric authentication and working on the Ethereum blockchain network[34].

"The real business case lies with merchants – increasing sales conversion rates and faster, more convenient payments at the checkout. In e-commerce, the checkout process is extremely challenging. Merchants are still experiencing up to 30% drop off of customers that don't complete their purchase. We want to help them increase conversion rates."

Claus Richter, *Head of Cash Management Customer Solutions at Nordea Bank.*

[29]
[30] www.fortune.com/2015/03/17/alibabas-jack-ma-shows-off-new-pay-with-a-selfie-technology/
[31] www.usatoday.com/story/tech/news/2016/03/15/amazon-files-patent-pay-selfie/81808188/
[32] www.techcrunch.com/2015/01/06/square-cash-integrates-touch-id-to-send-money-using-your-fingerprint/
[33]
[34] www.findbiometrics.com/blockchain-biometrics-startup-silicon-valley-hq-406081/

Chapter 3.

ANSWERING THE CHALLENGE?

A well thought out strategy for implementing biometrics needs to consider the concerns of industry bodies, regulators and consumer-interest groups. This section sets out the primary concerns and the reality behind them.

In particular, with the growing awareness of the risk of cyberattacks, the consumer lens is clearly focused on data security. As more banks, financial institutions and technology companies implement biometric programmes, questions are emerging about potential risks or weaknesses – ranging from privacy concerns, to worries that biometric technology can still be compromised by spoofing or manipulation.

THE 'SURVEILLANCE' SOCIETY

Among the most commonly cited objections to biometrics is that they are part of a rise in society-wide 'surveillance' – particularly relevant to biometric data where, the case of face recognition technology often operates without individual consent.(Google chief executive Eric Schmidt even says that facial recognition was "the only technology Google has built and, after looking at it, we decided to stop"[35]).

Public-sector biometrics are particularly under fire. The Electronic Frontier Foundation (EFF), a digital rights advocacy group, has raised concerns about government's expanding use of biometrics at border controls without regulatory oversight, with high risk of 'scope creep', especially in the US context[36].

In India, the Aadhaar digital ID project started collating biometric information to curb corruption and distribute subsidies, but the programme swiftly became almost

"Privacy groups maintain that there needs to be more specific legal control over the use of biometrics to address not only information security risks but also protection of the rights of individuals when their biometric data is obtained for one purpose and then begins to be used for purposes beyond the expectations of privacy of individuals."

Robert Bond, *partner with law firm Bristows.*

mandatory. As it links up to private institutions, including banks and credit checking firms, the government is accused by some of providing an inadequate legal framework to protect citizens' privacy, which leaves corporate use of the database unregulated. NGOs fear that private companies could ultimately access government-held personal data in the Aadhar system, such as medical records, while the government could use company data to target individuals in their campaigns[37].

THE "HONEYPOT"EFFECT

Biometrics could create a 'honeypot' in which a breach has catastrophic consequences because all of the valuable information is accessible from one entry point, versus a complex system that offers less convenience but is harder to hack.

Stores of physiological or behavioural data are a potential goldmine for hackers, who could use the information to access accounts or steal identities. A serious attack could impose huge costs and reputational burdens on financial institutions whose success, and business, depends on trust and security.

In the case of Equifax, one of the largest holders of financial information in the US, which was recently hacked. "If you were not only storing credit details, but biometric templates, you would now have exposed a massive chunk of America's population's biometrics," says Veridium's Mr Stickland. "Imagine your fingerprints, your irises, your face, your voice. You don't get to recreate that like you would a password. There's a complete dependency on the right degree of security."

Biometric templates cannot be reverse engineered easily or accurately e.g. to re-create the person pictures or voice print so this provides one level of protection. In addition, multiple layers of security including industry best practice encryption methods and hardware security modules underpin the overall security of the system including both the transmission and storage of biometric template data.

In terms of usage, since implementations are multi-factor they include use of private keys per user, device binding, silent authentication, collecting of device signals (to detect if a device has been challenged in some way) and anti-replay of biometric defenses, a compromise of all these mechanisms would be required in order to use the biometric templates if actually stolen. The authentication system would detect a security challenge and that someone was attempting to replay stolen biometric template data.

In order words, biometric data would be very hard to steal and even then it is highly unlikely the actual biometric data could ever be re-created from stolen biometric templates and even less likely it could be used to perform a transaction without hacking the overall security of the authentication system in the first place.

SPOOFING

Biometrics are clearly less prone to theft or fraud than passwords. Fingerprint scanners can now detect a pulse, and facial-recognition software such as iProov's and Apple's can measure depth of field, making it harder to fool systems with photos. Yet these systems are still fallible. Mr Bud describes spoofing as the "critical and central problem surrounding biometrics".

Researchers have broken into Apple's Touch ID system using Play Doh and conductive ink[38]. Twins tricked HSBC's

voice verification system; and a security researcher in Berlin photographed his friend's iris and affixed it to a contact-lens to prove that Samsung's Galaxy S8 scanner couldn't tell the difference. Mr Bud, whose company was established to tackle the spoofing problem, recalls testing one bank's "first generation" face verification software. It took them 2.5 minutes to break. Against this kind of backdrop, surveys suggest that some customers neither trust nor understand biometrics, and may prefer to stick with the status quo. In a count of 12,000 people across 11 countries, for example, HSBC found that less than half trusted fingerprint recognition over passwords[39].

Some financial institutions have been deterred by these risks. "When they started testing them, they found that they could spoof them with very little effort, and they said: 'What use is a technology which I can spoof so readily?'," Mr Bud argues. For the same reason, those which have deployed biometric technology are often cautious of using it for high value transactions. Mr Bud recalls telling the managing director of the bank that his system was easily penetrable: "He wasn't particularly bothered. He said: 'We know it's not particularly secure so we don't allow people to do anything serious with it.'"

Mr Bud believes the issue is being taken more seriously now. "Until about a year ago the market really was not very sensitive to this idea of spoofs. It regarded it as a secondary product feature," he argues. "In the last year we've seen a change, with banks investing a significant amount of money to evaluate the spoof performance of biometric technologies.The market has moved a long way towards an understanding that spoof detection is the key requirement for allowing biometrics to be used in the sorts of applications where they are most needed."

WHO HOLDS THE DATA? AND WHERE?

The location where biometric data is stored and whether it can be hacked is another key concern. "The issue of keeping data secure is what consumers are concerned about," notes James Moar, senior analyst at Juniper Research, a UK-based digital market specialist. "The banks are very keen to point out that the data is stored in a secure enclave… but getting the consumer to understand those and have faith in those is quite a challenge. There's that lingering concern over what happens if my fingerprint gets stolen."

"Biometrics are great security tools as long as you can control the data," says Sarah Jane Hughes, fellow in commercial law at Indiana University, who has testified to US Congress Committees on how to regulate biometrics[40]. She argues that an essential protective layer involves adding complexity to data storage. "If we can somehow silo the data - keep biometrics in one place, transactional activity in another place, and some other authentication information in a third place - that would help".

To protect data, banks have a choice between two options: conduct biometric authentications over the device, and trust the hardware manufacturer to securely store the information, or do so over their own networks. These approaches "address two different sources of risk, and it depends which you take more seriously," Mr Bud explains.

Centralised data is encrypted and kept in secure databases which are accessed through tokenisation. "There's a good deal of technology that can ensure that those details are securely stored," notes Juniper Research's Mr Moar. "I'm happy to put my face in front of a camera, have it transferred through a bunch of algorithms, and have it stored deep in a database." Mr Holden at Atom Bank says. "We have rigorous access control that sits around all our data."

Centralising information confers an advantage: where breaches of personal phone security might go undiscovered, banks which store information centrally can observe and defend attacks. "If you are worried about biometrics giving rise to a security risk, then you must do it over the network, because you can learn from their attacks and present a moving target. You can maintain resilience over time," Mr Bud argues.

Those who want to avoid central custodianship prefer to conduct authentication using the device, as most fingerprint scanners do: "You put it all in the hands of the end user and let them be the ones accountable", Mr Stickland explains. When a phone registers your fingerprint, it stores the data as a mathematical template in a secure part of its memory or on a remote server, and then compares your next touches against the snapshot. So long as those are secured or encrypted, it is difficult to re-create.

Yet spoofs prove that this system is fallible too. Since both have their limits, a debate over the best method of storing biometric data now divides financial institutions. "There are some, particularly in the US, who are passionate about on-device biometrics, and they are the supporters of fingerprint ID," Mr Bud argues.

Gemalto has designed a tablet that immediately stores the fingerprint on the card sensor. At first customers will need to go to the bank branch to register their fingerprints but Gemalto is working on self-enrolment solutions for use at POS or at home.

Mr Stickland believes that there is a "third way": Veridium has patented technology which co-locates biometric information. "As people better understand the use of biometrics, they will argue that both localised and centralised systems are fallible," he says. "Why wouldn't you co-locate an encrypted, fractured piece of your template, so that no one piece can be re-created? If you can build it like Harry Potter's Horcrux… it's far harder for anyone to then hack you."

"The fingerprint is transferred onto the card and nowhere else, This puts the cardholder in control and there is no other database that can be hacked."

Sylvie Gibert, *SVP Payment Cards, Gemalto*

[35]www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/
[36]www.eff.org/de/issues/biometrics
[37]www.theguardian.com/sustainable-business/2017/feb/09/fingerprint-payments-privacy-fears-india-banknotes
[38]www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/
[39]www.ft.com/content/012f9b52-3fcd-11e7-9d56-25f963e998b2
[40]www.biometricupdate.com/201512/congress-investigates-security-of-mobile-payments

Chapter 4.

PREPARING TO LEAP

Adoption of biometrics in consumer technology and financial services has gathered momentum across multiple regions. The benefits of greater convenience and added security, improving technological accuracy, and their simplicity relative to alternatives, are increasingly recognised by vendors, financial service providers and consumers alike.

There are still obstacles to overcome. Realising the potential of biometrics to connect the last link in the payment value chain requires not just an answer to these challenges but a strategic approach that aligns the interest of customers, ecosystem partners and merchants to drive adoption and acceptance. This chapter summarises best practices and key considerations for financial services companies, technology vendors, consumers and governments.

CONVENIENCE AND SECURITY ARE DRIVING ADOPTION BY CONSUMERS, ACCEPTANCE AMONG MERCHANTS

In the digital age, user experience is essential. When it comes to logging on to bank accounts, paying for a sandwich, or transferring small sums to a friend, customers expect services they can access without friction. The greater the convenience that biometrics can offer, the greater the adoption and use of more of the product or services. As consumers grow more comfortable with the tools, for instance through quicker processing at airports, calls for more widespread use of these technologies are likely to get louder.

By enabling faster transactions at the check-out, or easier payment online, biometrics can bring great value to merchants, growing the market for electronic transactions in the process, “[in-store] half a second is as much time as you’ve got,” Mr Bud says. “Anything longer and people say: “To hell with this, it’s too hard.” Mr Tyler at Westpac argues that this is why fingerprint technology has been so popular: “Fingerprint has been around for three or four years now, but to this day it’s one of the main things our customers like about our app.” The first reason for that, he says, is that “we’ve taken away the friction… The convenience is so critical.” Similarly, voice authentication in telephone banking is popular because it feels “very much natural”, he says.

Biometrics do not always provide optimal convenience - some solutions fail to deliver with ease. Mr Moar notes that iris scanners such as Samsung’s or Mastercard’s facial recognition system take too long. “It doesn’t feel frictionless enough to see a wide adoption,” he says. “As much as consumers want security they also want convenience, and if it’s going to be a pain, they won’t use it.”

False readings are another problem. “When it comes to mobile banking, it has to work 99.999% of the time,” Mr Tyler says. “And some of those new mechanisms are quite early stage. If it becomes that I can just open my phone and I’m in, then I’m up for it. If it fails one in ten times, I’m going to default back to a more reliable and fast mechanism.” He argues that face, voice and iris recognition “are the next evolution in biometrics, with these types of mechanisms gaining widespread adoption, most notably with Apple launching Face ID on the new iPhone X.”

COMPLEXITY PAYS, SOMETIMES

Convenience may not always be the priority. For more important transactions, such as setting up a new payee, changing an address, or transferring larger sums of money, users recognise the need for greater security and prioritise ceremony over speed. “If it’s a simple quick, low value transaction then you’ve got to be fast above all. So an idea has grown up in the industry that speed and frictionless-ness is everything,” Mr Bud says. “But when customers are doing something that they understand is risky, they want to be sure that you are protecting them. If you make it too fast and frictionless, they worry. If it’s a more serious transaction, then fast is bad, ceremony is good. That’s something that the industry needs to get its head around.”

“There are interactions where customers want some friction,” agrees Mr Tyler. “If I’m sending a large amount of money, and we didn’t have a second-factor authentication in place, customers would say: “I want to be challenged on that amount of money”.”

Mr Ram says that HSBC, which is prioritising its biometric offerings for commercial rather than retail customers, is focused on security over speed. “A large part of our role is that the customer wants to be secure… [They’re] not worried about their users having to take an extra step if it ensures that we provide an appropriate level of security,” he explains.

A related challenge concerns back-ups for these more convenient tools since any transition to a new technology carries risks. “If you do have any issues with your upgrade, you’ve got to really think about the fall-back mechanism for people to still access their banking,” Westpac’s Mr Tyler notes. It found that when fingerprint scanners failed, customers had often forgotten their old credentials. “When you’ve made something so simple and seamless, if something fails you need to look at how you are going to recover quickly,” he says. “We’ve made sure we had graceful failover”, which means that the system defaults back to easily-recalled pin codes where necessary.

BIOMETRIC AUTHENTICATION BENEFIT FROM A HALO EFFECT WHEN DRIVEN BY THE WHOLE ECOSYSTEM

Biometrics are not being spearheaded by either the private or public sector. They are flourishing thanks to broad-based usage that includes technology companies, governments agencies and financial services companies. This normalises the technology across different use cases and gives greater consumer comfort. Public transit systems like Transport for London (TfL) normalised contactless card payments, driving a shift in consumer behaviour which increased people’s trust in alternative payments, and encouraged adoption by merchants and retailers.

Similarly, passport control services are increasingly using biometrics at national borders to reduce queuing and processing times, contributing to a halo effect - making consumers feel more comfortable as they trust the public sector entities in a way that would take longer from the private sector. “The adoption of biometric mechanisms in the public sector and military has been paramount to us, mainly because of the sheer volume of usage,” argues Mr Holden at Atom Bank. “We recognised where these things were being used and are learning from their learning, using [these] examples… has been crucial for our customers.”

In some countries, governments have also developed national biometric databases, which can be leveraged by financial institutions. India’s collection of the fingerprints, photographs and iris scans of more than a billion people under Aadhaar was followed, this year, by the Reserve Bank mandating that all its financial institutions adopt biometric authentication. Mr Stickland notes that Mexico and Brazil collect individuals’ biometrics when they vote, or register for an identification document or driver’s license. “Banks are benefiting from that because they can use that information to validate individuals for anti-money laundering purposes,” he says. “The uptake is huge.”

BIOMETRICS CAN SAVE COSTS AS PART OF THE SHIFT TO DIGITAL AND MOBILE BANKING

Though they require some investment, introducing biometric technology can eventually be cost-saving, argues Mr Stickland. “At the moment, you have lots of plastic: credit and debit cards and you’re carrying all these tokens around. That is probably costing Barclays £35-55 million a year, just in printing plastic and sending you tokens when you lose them,” he says. “Imagine if I could completely eradicate that from your bottom line, and secure your processing using existing hardware at the same time.”

Mr Moar at Juniper Research notes that the added security of chip and pin authentication reduced insurance premiums for financial institutions as signatures were phased out. “We’re not at the point yet that biometrics can do that for payments,” he says. “But when that lands, that’s going to be the main driver, as far as I’m concerned, for banks.” And Clive Bourke, President of EMEA & APAC at Daon, says that by driving more use of mobile, biometrics could help reduce in-branch banking and the need to maintain a large physical footprint.

Also addressing the issue of cost, is Hitachi High-Technologies, a subsidiary of Hitachi Corporation. Mr Ichiro Matsuba, General Manager of Electronic Components and Materials, acknowledges that, although customers understand the benefits of biometric authentication, the initial cost is still seen as a high burden. To encourage customers to launch new biometric technologies, Hitachi High-Technology has developed a range of pricing models, including leasing and an operating expense model, among others.

OPERATE A MULTI-LAYERED APPROACH TO AUTHENTICATION

Even the most ardent biometric evangelists acknowledge that banks should offer different biometric or non-biometric authentication methods, or require a combination of those - known as “multi-factor” - to boost security and convenience. “Good security relies on a multiple-layered approach,” notes Mr Holden at Atom Bank.

This is partly because biometrics each have strengths and weaknesses. Finger recognition fails when it is wet (and for a small portion of the population whose prints are unreadable). Voice recognition is not suited to noisy environments or contexts in which privacy is sought but not available, like open plan offices. And facial recognition systems can fail when it’s too bright, too dark, if a user is moving, or if they wear spectacles or grow a beard. This means that banks have to offer a pin or password which they can fall back on when biometrics fail, which undermines security gains. For this reason, some banks now offer their customers a choice between authentication methods, according to where they are, and what is most convenient.

Daon’s Mr Bourke argues in favour of offering multiple choices for consumers, including - but not limited to - biometrics. “We advocate offering a non-biometric authentication method in any channel you’re supporting, so the customer can choose a non-biometric authentication method. You’re giving people consumer choice and letting them decide,” he says. “There are still lots of people who do not have fingerprint technology enabled on their phones, and you don’t want to alienate that user group by saying that [is the only option].”

Increasingly, financial institutions also require users to conduct multi-factor authentication for higher-value or new transactions. And the forthcoming European Union’s Second Payments Service Directive, or PSD2, will enforce strong customer authentication protocols based on both something the customer ‘is’ and something they ‘know’.

HSBC, for example, will roll out a choice of biometric services in the near future, “so we can customise services in each market”, Mr Ram says. “Regardless of whether you’re making a $5 or 5 million-dollar payment you need to go through two factor authentication now, but what we’re trying to see is if there’s a biometric angle here to make it simpler. Depending on risk for that activity we want to be able to provide different options,” he explains. “Transactions are highly sensitive operations so we probably need more than one form of biometric authentication, plus one which is not biometric-dependent.”

Mr Stickland agrees. “We know that my fingerprint is not enough. The only way to really be secure is to use a multi-factor,” he says. He believes that the highest iteration of that technology is a combination of “implicit”, or behavioural biometrics, and “explicit” ones such as a fingerprint or iris scanners.

iProov’s Mr Bud similarly argues that multi-factor verification can improve security. But “you have to make sure that if you do have different methods, they aren’t just different ways of testing the same thing,” he suggests. The best methods combine one technology which “depends on the ownership of the mobile phone, which might be a fingerprint, or a piece of information stored securely on the mobile phone” together with “another method like in network face verification which is independent of whether the mobile phone has been cracked”. Do that, he says, “and your system is very secure”.

“Consumers demand choice, and if you offer multiple biometrics, they can choose which type to use,” explains Daon’s Mr Bourke. “If you pick a single type it might be that their device or environment doesn’t lend itself well to that”. As early as 2014, USAA started trialling a platform from Daon which offers users the choice of logging in using fingerprints, voice or facial recognition, according to where they are and what is most convenient. Today, over 2.5 million people are using USAA’s mobile app to access a full range of banking services with biometrics.[41]

“[Our commercial customers] are not worried about their users having to take an extra step if it ensures that we provide an appropriate level of security.”

Siva Ram, *SM, Information Security and Fraud Risk, HSBC*

ADOPTION WILL GROW THE NUMBER OF AREAS WHERE BIOMETRICS CAN BE APPLIED

Mr Ram notes that HSBC’s biometric trials have simplified the transaction process for commercial clients. Mr Bud agrees that biometrics have further to run in commercial banking. “Credential compromise is quite an issue in the commercial banking area... large amounts of money can be defrauded,” he says, adding that biometrics can also help to secure supply chains. “In supply chains, in areas like mortgages and lending, you have banks dealing with brokers, dealing with resellers, and increasing there’s an obligation to ensure that all the information which travels up and down the supply chain is protected… Biometrics are a very good way of doing that.”

Mr Stickland expects to see a greater use of biometrics within banks’ trading arms, by treasurers, and within the insurance business. “Many capital markets firms are looking to biometrics to help them validate the individual trader to the transaction, in order to prevent fraud. Trading with an explicit authentication using face, voice or fingerprint is becoming a working practice,” he explains. “Treasurers can have one banking app where they move funds rather than having to carry 26 tokens around”. Meanwhile biometrics can make false identity claims in the insurance industry “a thing of the past”: “Suing your doctor or prescriber of drugs will be eradicated, because you will biometrically validate who you are, when you receive your drugs,” he argues.

ENGAGE IN EDUCATION, DIALOGUE, TRUST-BUILDING

As criticisms of biometrics emerge from privacy groups and consumers, active dialogue about the risks and downsides is critical. “As soon as the digital space is involved at all, there’s a sizable group of consumers who are going to be sceptical of the whole thing,” Mr Moar says. “It’s a matter of reassuring consumers not so much about what the security measures are, but how they will impact them and how secure they are compared to other measures.”

Biometric companies can do more to address concerns about biometric data being ‘stolen’ and ensure consumers are properly informed about how biometric tools work. “These systems are not designed based on the fact that your biometric is a secret,” explains Mr Bourke at Daon. “We expect and know that your face is on Facebook and LinkedIn, that there are potentially videos of you somewhere online, and in fact we assume someone may try and perpetuate fraud by using photos or video. The premise is that there is at least one other factor of authentication, e.g. using the device and more factors can be combined if necessary. So it has to be a combination of your face, in a live scenario, with your device and alternative factors to log in to something – and that data only opens the front door, we may assess more factors to allow transaction approval”.

Since banks’ reputations depend on their ability to protect customers’ assets and data, they prioritise technologies which are secure, and need to ensure their customers understand biometrics are designed to improve security, not compromise it. “Security is the first thing I think about. With biometrics you want to make sure that the spend - because it’s not particularly cheap - is going to give you the best security mechanism for your money”, says Mr Holden at Atom Bank.

”Société Générale added an annual subscription fee for this feature and the bank has had 200,000 applications for it, and a significant proportion of them from new customers. The fact that consumers are clearly willing to pay for more features indicates that banks can attract new customers with new, innovative products and features – including biometrics.”

Sylvie Gibert, *SVP Payment Cards, Gemalto*

“The security element is really important.” Travis Tyler, Westpac Group’s General Manager for Consumer Digital, agrees. “Everything we do has to be secure, first and foremost,” he argues.

“Building trust around a new form of security was really important to us… Reassuring people that this is a secure way of protecting your account and money,” says Mr Holden at Atom. His bank found that using examples of public deployment of biometrics helped to reassure customers.

Coaxing users to improve their own practices is also important, regardless of login and authentication methods. “When customers register their biometric security, we prompt them to make sure that their phones are locked, and there’s a key or fingerprint lock on the phone, so you’ve effectively got two factor identification: to the phone and to the app”, explains Mr Holden. Westpac’s Mr Tyler agrees. “The most important part is making sure our customers are protecting themselves,” he says: “Making sure that they’re not sharing passwords, or using public Wi-Fi to login, and not sharing information if they get an email asking for their details.”

TEST THE TECHNOLOGY, MONITOR USAGE, AND REFINE (REPEAT)

Test the vulnerability of biometrics to weed out potential flaws and weaknesses. “If you’re serious about using a system, pay a hacker to attack it hard,” Mr Bud says. “It’s extremely important to treat the hackers with respect and to probe the vulnerabilities…. if you underestimate the opposition you will sooner or later end up being very badly hurt.”

After adopting new technologies, financial institutions should also monitor uptake, preferences and use by different demographics. For instance, Bank of America recognises that some people are concerned about biometric security, so it studies other companies, both inside and outside the financial industry, and is learning what consumers want.[42] More often than not, banks test new offerings in small internal pilots which are sometimes followed by larger customer tests, allowing them to gauge understanding, usability and design, and to make amendments before they roll out the technology to all customers.

Atom Bank started planning its app in 2014, then sent it live in a controlled deployment in April last year. After registering customers’ devices and identity credentials, it lets them choose whether they want to log in to its app using face, voice or passcode. Citibank’s app offered five methods of authentication for wealth management clients - fingerprint, voice, facial recognition, PIN, and traditional password. The bank developed the service internally and tested it on 2,500 clients over five months in order to refine its design.[43] “You learn much more from user reaction and in-field performance than you do from any number of specification studies or background studies or paper reviews,” says Mr Bud. Gemalto’s Ms Gibert points out that a lot of work is still being done to ensure biometric technology meets appropriate quality requirements, and that standards are in place. In payment cards, deployment will come after successful pilots. “We will only see large-scale deployments in 2019, not before. Every part of the value chain has to be ready, the technology perfect, and all players in compliance with every one of the requirements.”

BEWARE TECHNOLOGY ‘LOCK-IN’ AND DEVICE-DEPENDENCE

With so many services accessed on mobile there is a natural disintermediation at play in which device manufacturers and technology companies are the ones developing the technologies themselves. Mr Goode says that banks are tending “to use biometric vendors and authentication security companies that have adopted biometrics into their authentication platforms. I’m not really seeing them build out the systems themselves.

“In this new environment, success comes by working with the whole ecosystem – partners are really important. The market is quite rigid so you need to activate the whole value chain, share the upside with partners, and foster a collaborative environment,” says Zwipe’s Mr Humborstad. “Some companies have a ‘you win, I lose mindset’. You have to create a win-win scenario. As Zwipe, we can’t get the product to market if we can’t work with the card schemes and they can’t get it to banks which means everyone loses out.”

Collaboration does however raise questions as to “the chain of liability”, argues Mr Bud. “Banks have been extremely cautious about allowing biometrics to do much more than gain visibility access and do payments and transfers to already established payees,” he says, partly because they fear “putting their destiny in the hands of businesses with track records that don’t stretch into the decades.” He explains: “Some of these technologies require them to trust completely another vendor or chain of vendors, without the vendor indemnifying them. That’s not something they were [all] willing to do.”

Juniper Research’s Mr Moar explains: “If you’re looking at an Android-based system, for example, it can be difficult because you can’t guarantee that whoever is making the hardware will have that secure element to keep biometrics safe.”Mr Ram notes functionality concerns. “The challenge with biometric methods is the reliance on third party technology. It could be difficult to determine where the problem lies if the transaction isn’t authorised or the solution doesn’t seem to work,” he says. As far as commercial banking goes, HSBC’s Mr Ram notes that many companies shirk the use of mobile phones entirely. “Some companies… are actively stopping users from using mobile, as it’s perceived too risky,” he says. “The challenge we see is: Whose phone is it? If you’re an employee of a large company you’re transacting on their behalf – whose phone is it? When it comes to security on mobile, the question is: How do you bind the mobile phone to the user?

Some financial institutions prefer to store biometric information on the device, as Touch ID or Apple’s FaceID does, and others prefer it on their own network. “This addresses two different sources of risk, and it depends which you take more seriously,” Mr Bud says. “If you are worried about biometrics being seized and published then you prefer biometric solutions on the device. But if you are worried about the security of the system, and the biometrics giving rise to a security risk, then you must do it on the network. If you put it in the network you can observe them attacking you, learn from their attacks and present a moving target. You can maintain the resilience of a system over time.”

The research shows that device-specific approaches do worry financial institutions. “In terms of banking apps and payments, the uptake of biometrics depends an awful lot on the devices that are being used,” says Juniper Research’s Mr Moar. While Apple led in the deployment of biometric hardware on mobile phones, Samsung and other Android manufacturers are making up ground. As Westpac’s Mr Tyler notes “some of the manufacturers didn’t get the experience right, so it was a bit slower.” Although those manufacturers have now embedded sensors on flagship and some mid-range phones, there are still “a lot that don’t have fingerprint scanners”, Mr Moar says.

Many solutions, such as facial recognition on the new iPhone, or iris scanning on Samsung’s S8, are available only to a select group of mobile-owners, which can provide a communications challenge for banks. Westpac’s Mr Tyler observes that after it started offering fingerprint scanning to iPhone users, “We had pretty strong feedback within a couple of months from Android customers who were asking: “Where’s ours?” Moreover, most tablets, laptops and PCs are not embedded with sensors to read fingerprints or eyes, meaning that solutions can only be taken up by those who bank or shop on their phones.

In order for biometrics to be mainstreamed, this era of device-dependence must draw to a close. “We need to make sure that people select hardware agnostic solutions – so software-driven outcomes,” Veridium’s Mr Stickland says. “What we don’t want is to rely on Apple or Samsung’s latest release to be able to make these things effective. We need them backwardly integrated into phones and computers of 2000, as well as the future.” He believes that a degree of standardisation is required. “The industry

as a whole is struggling with standards: how many different options can we support? We need to decide the type of equipment we can support and need to land on something that is pretty standardized."

Solutions with broad applicability are already available. Almost all devices are now equipped with a front-facing camera, making technologies such as Mastercard's pay-by-selfie available to any smartphone user, and allowing banks to onboard customers through their laptop. The introduction and deployment of biometric smart cards will leverage existing infrastructure to create traction and mass deployment. Clients can use any phone to authenticate themselves by voice. "One reason that banks are so fascinated by face biometrics is precisely that it's the one data rich technology where you've got the sensors everywhere now," Mr Bud says. Mr Stickland notes that Veridium's technology requires only a 5 megapixel camera. "You can make a deployable solution on existing infrastructure," he says. "But you still have to go through the customer education process."

REGULATION IS PLAYING CATCH-UP

Regulators are only now beginning to put in place frameworks governing biometrics. In the European Union, biometrics had not been defined in relation to personal data until the EU General Data Protection Regulation (GDPR), which specifically identified biometrics as a special category of data (sensitive personal data) demanding greater protection and more specific permission from data subjects. GDPR defined biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that person, such as facial images or dactyloscopic data."

"If biometric data is being processed by a business or a government agency there are specific obligations under GDPR as to the information that has to be given to individuals in relation to that processing as well as the lawful grounds for processing and continuing to store that biometric data," says Mr Bond at Bristow. "Whilst GDPR applies protection for the rights of individuals in the biometric data, it also imposes on businesses that use biometrics [the need to be] more transparent and more accountable about the way in which that biometric data will be processed".

European regulators are also catching up on customer authentication rules. The European Commission's Second Payment Services Directive (PSD2), which comes into force next year, includes a new rule called the Regulatory Technical Standard (RTS), which lays out standards for secure customer authentication. Its draft was released in early 2017. "The whole of 2016 was spent consulting and arguing about what the RTS was going to say, and the banks really couldn't do or plan anything until they saw how that was going to pan out," iProov's Mr Bud says. "The definition of what would be considered acceptable means of authentication under PSD2 was up for grabs. That has set the rhythm for decisions about changes in authentication: there was no point in banks playing around when the end timing wasn't clear."

In the US, says Professor Hughes, there has been little regulatory updating. Multiple agencies are engaged in different aspects of biometrics: the National Institute of Standards and Technology has long been evaluating biometric identification on face identification, fingerprint, voice, and iris scans, while the Federal Trade Commission leads on aspects around data security, and the Department of Health and Human Services handles personal health information[44]. Professor Hughes worries that the US regulatory system is not as strong as Europe's when it comes to data. "We [in the US] do not have great rules about with whom data can be shared". Relevant legislation, including the Electronic Communications Privacy Act (1986), the Privacy Act (1999) and the Patriot Act (2001), have been little updated for the biometric era. "The ability of companies to use data they receive, and to share it with others, is more restricted and to send it outside the country - which complicates cloud computing - is very much more regulated across the European Union".

HSBC's Mr Ram notes a final regulatory challenge: compliance with variable international regulations. "We have to comply with 60+ regulators and regulations," he says. "With retail banking it's simpler as the app can be customised at the country level. Corporates, in comparison, are in multiple countries and we need to make sure we comply with each regulator in each market, and then that the app works across borders." He gives Asia as an example: "Asia doesn't want transactions above $50,000 authorised by biometrics. This wouldn't be much of an issue for personal banking but for commercial banking this is a challenge... So we need to look at it at the country level."

[41] www.findbiometrics.com/usaa-app-biometrics-revolution-403171/
[42] www.americanbanker.com/news/the-eyes-have-it-bank-of-america-samsung-pilot-iris-scan-logins
[43] www.finextra.com/newsarticle/29883/citi-fintech-unit-taps-agile-methodologies-to-craft-new-mobile-app
[44] www.papers.ssrn.com/sol3/papers.cfm?abstract_id=2640607

The Biometric Decrypted Report

a comprehensive global pulse check on the latest developments and deployments of biometric authentication solutions in payment, was carried out between August and November 2017 utilising comprehensive desk research and interviews with 15 leading international experts from banks, solution providers, analysts and academia.

AUTHORS
Adam Green, Eleanor Whitehead,
Simon Hardie from
MagnaCarta Communications