REPORT | AUGUST 2017

Biometrics in Digital Financial Services: An Overview

REDUCING POVERTY
THROUGH FINANCIAL SECTOR DEVELOPMENT

consult hyperion
securing tomorrow's transactions

fsdafrica

Key points

01

A biometric can be used for identification, as an identifier to reference an individual user's identity (1:n matching), and for verification, to help authenticate that a service user is who they claim to be (1:1 matching).

02

Biometric identification (1:n) is one of the few mechanisms that can recognise that an individual is duplicated on a service, if this is a requirement of the service. Identification using a biometric is often time consuming and expensive. To correctly register the individual, capture a unique biometric and link it to the customer account can be complex.

03

For financial services, biometric technologies tend to have more applicability and are increasingly being used for customer verification (1:1). In combination with other authentication factors, biometrics are most commonly used for access control to services (i.e. to logon to an account) and authentication for transactions (i.e. payments).

04

Biometric technology aims to achieve a balance between security, convenience and transaction speed for a range of applications. This balance is important for financial service applications, especially retail payments, where risk management needs to be balanced against convenience and transaction speed at a point of interaction.

05

The accuracy and reliability of a biometric depends on the type of biometric and the tuning of the system used to capture it. Not all people will be able to use a particular biometric and so multiple biometric types or alternate methods are required to ensure individuals are not excluded from a service.

06

Customers require low cost, convenient and reliable verification methods, using an approach that offers appropriate speed for the transaction being performed. Banks require straightforward systems for low cost enrolment and customer management, using a biometric that offers a level of security appropriate to the action being undertaken.

07

For the mass market, mobile phones, in particular smart phones, are the platform of choice allowing voice, face or fingerprint recognition to be used. The choice depends on the capabilities of the user's device and the environment in which the service is used.

08

This study suggests that most financial service and payment applications using biometrics do so for strong authentication, as part of customer verification for access control or payment initiation, not as part of customer identification processes. Biometrics can play a key role providing ease of use and convenience when used as one of a number of authentication factors.

Biometrics in Digital Financial Services: An Overview

BY: DICK CLARK

Contents

List of Figures & Tables

Acknowledgements

"Biometrics in Digital Financial Services; An Overview" was authored by Dick Clark, Principal Consultant at Consult Hyperion. He would like to extend his gratitude to the U.K. Department for International Development (DFID) and Financial Sector Deepening Africa (FSD Africa) and to the following for assisting in compiling the report: Paul Makin, Iain Brougham, Joe Huxley, Fundi Ngundi and Martin Namasaka.

The views expressed in this report are those of the author, Consult Hyperion, and in no way entirely reflect those of FSD Africa.

Executive Summary

This paper presents the results of a focussed, independent analysis of biometric technologies, and considers their application and acceptance for retail payments and conventional financial services for people in emerging economies. In particular, we consider the application of biometrics technologies for population-scale deployments in the retail financial services sector.

A biometric is a representation of a characteristic of a person, such as fingerprints, voice, face, or iris patterns. A biometric can be used (usually as one of a number of factors) for two functions:

Identification
– to identify an individual within a population, helping to answer the question "Who is this person?" Referred to as 1:N matching.

Verification
– to authenticate that the service user is the individual the user claims to be, helping them claim "I am person X". Referred to as 1:1 matching.

Customer identification is a key regulatory requirement within financial services, often referred to as Customer Due Diligence (CDD) or Know Your Customer (KYC). Most markets have KYC and Anti-money Laundering (AML) regulations that require identification of customers to specific standards, and usually require a reference to a government issued identity (where it exists). A biometric can be used as an identifier linking to an individual's identity. The accuracy and reliability of the biometric identifier depends on the type of biometric and the tuning of the system used to capture it. Biometric identification can help reduce the likelihood that an individual customer is duplicated on the service, if this is a requirement of the service.

However, identification using a biometric is time-consuming and expensive, as it usually requires manual processes to register the individual, to capture the biometric and link the biometric to the customer account. The quality (the uniqueness) of the biometric captured can depend on the skill of the person performing the customer registration and there are several examples of notable national identity schemes using biometrics with well publicised quality control problems[1].

It must also be recognised that not all people can use a particular biometric and that alternate methods are required to ensure individuals are not excluded from a service. For two of the most widely used biometrics, the typical failure-to-enrol rate (as measured by IBG[2]) indicate the difficulty of using technologies on a population scale:

- For fingerprint: in every 1 million users there will be 25,000 people (2.5%) that cannot be enrolled[3];
- For finger vein: in every 1 million users there will be 800 people (0.08%) that cannot be enrolled.

To overcome this problem multiple biometrics may need to be captured. In India, the national identity scheme, Aadhaar, captures a range of biometrics (ten fingerprints and two irises), to ensure uniqueness during enrolment and increase the chance that identification will continue to be accurate over time. Once these are captured, an Aadhaar identity number is issued. To access services, users present their Aadhaar number, and that is used to access an online service (remotely) to check their biometrics for verification.

[1] http://www.theguardian.com/global-development-professionals-network/2016/feb/22/biometrics-aid-development-panacea-technology
[2] http://l.b5z.net/i/u/6084428/i/CBT7_IBGReport.pdf
[3] This applies to the general population. It may be higher if choose for an inappropriate set of target users.

It is worth noting that probably the most significant application for biometrics technology worldwide is the electronic passport (ePassport). Globally, there are 100s million ePassports in use, each containing a chip that stores an image of the passport holder. These have been deployed internationally with a high degree of interoperability, achieved through standardisation. This degree of standardisation and interoperability is not present for the use of biometrics in financial services, including mobile money applications.

For these reasons, it is likely that financial services organisations will continue to rely on third party identification for CDD in most applications. For financial services, biometric technologies have more applicability and are increasingly used for customer verification. Once a customer is identified to a service, a service user can enrol a biometric allowing the service to use it to link the user to the customer account.

In combination with an account identity, and other authentication factors, biometrics are used for customer verification for:

- Access control to services – using biometric for authentication and logon to account services for banking and payments, such as over the internet or at an ATM;
- Remote internet or local in-store payments – using a biometric during a payment transaction that can be accepted over the internet or at a physical point of sale. This requires the capture and matching of the customer's biometric during the payment process and so may have taxing performance requirements to ensure usability.

Biometric technology aims to achieve a balance between security, convenience and transaction speed for a range of applications. This balance is important for financial service applications, especially retail payment applications, where risk management needs to be balanced against convenience and transaction speed at a point of interaction.

Customers require low cost, convenient and reliable verification methods, using an approach that offers appropriate speed for the transaction being performed. Banks require straightforward systems for low cost enrolment and lifecycle management, using a biometric that offers a level of security appropriate to the action being undertaken.

Different technologies and different solution architectures address these in different ways. Corporate applications have been deployed using finger vein biometric readers for access control to internet business banking. For the mass market, mobile phones, in particular smart phones, are the platform of choice allowing voice, face or fingerprint recognition to be used, depending on the capabilities of the user's device and the environment in which the service is used.

As ease of use is seen as more important than accuracy for the mass market, the tuning of the biometric solution is such that the occurrence of false rejections is designed to be low. False rejection is when verification fails even though the person being verified is the correct person. Tuning the system to reduce the likelihood of false rejections increases the likelihood of false acceptances – the likelihood the wrong person gains access to the service in impersonation of another person. This means that, while there is a clear perception among the public that biometrics can solve identification problems and offer added security, for these solutions the strength of the security is not from the biometric but from the system as a whole. For mobiles, this means services must verify the integrity of the mobile device itself to ensure strong authentication can be achieved.

Early deployments on mobile (such as US bank USAA[4]) reported that customers prefer biometric verification (particularly face recognition) to having to remember personal identification numbers (PINs), which has led to increasing support among global brands, including banks (for example, HSBC[5]) and card schemes (for example, MasterCard[6]).

For in-store payments, the customer verification is undertaken immediately prior to the payment transaction being submitted. Payment initiation may be via contactless interface to the point of sale (POS) terminal if the device is capable (for example, with Touch ID on Apple Pay) or over the mobile channel, provided an appropriate network is available. The research for this study did not identify large scale mobile money schemes using biometric verification, but there is no intrinsic reason why the initiatives used in more conventional payments cannot be applied.

This study suggests that most financial service and payment applications using biometrics do so for strong authentication, as part of customer verification for access control or payment initiation, not as part of customer identification processes. This is expected to continue as biometrics can play a key role providing ease of use and convenience when used as one of a number of authentication factors.

---

[4] http://www.americanbanker.com/news/bank-technology/biometric-tipping-point-usaa-deploys-face-voice-recognition-1072509-1.html
[5] http://www.bbc.co.uk/news/business-35609833
[6] http://www.cbc.ca/news/business/mastercard-selfie-pay-1.3459740

1. Introduction

1.1 Purpose

This document provides an overview and independent analysis of the applicability of different biometric technologies and their market acceptance within financial services and retail payments, with a specific focus on emerging economies.

The objective of the paper is to help the reader to understand the areas where the use of biometric technologies is of value to financial services and payment applications, and to gain an insight into the strengths and weaknesses of the various types of biometrics. The paper aims to help readers make an informed choice as to whether biometrics technologies may apply to their own application and which technologies they should consider investigating further.

1.2 Scope

The paper introduces the key types of biometrics currently in use and how they are may be applied to both mobile money and conventional financial services. This includes the various types of payment acceptance, such as in-store at POS, at unattended POS (for example, vending machines), or remote (Internet) payments using a PC, tablet or smart phone. Consideration is made for both mobile and non-mobile approaches.

1.3 Sources

The information collated and analysed in the preparation of this document has been obtained from publically available secondary sources. The sources for the information used are referenced, along with any relevant assumptions.

2. Overview of Biometric Solutions

2.1 Definitions

A biometric is a representation of a characteristic of a person, such as fingerprints, voice, face, or iris patterns. 'Biometric solutions' are the systems, processes, and technologies utilising biometrics for the purposes of identification or verification of individuals in different applications.

A biometric can be used as one of a number of factors for two functions: identification and verification. These functions are fundamentally different:

Identification is the process of identifying an individual within a population, helping to answer the question "Who is this person?" For example, a facial image of a person may be compared against lots of images in a database. Positive identification occurs if the person to be identified is found in the database. Negative identification occurs if the person is not found. Negative identification can be used for ascertaining if there are no duplicates in a database; useful, for example, to 'weed out' duplicate registrations. This process is also be referred to as 1-to-many or 1:N matching, or recognition.

Verification is the process of authenticating that the service user is the individual the user claims to be, helping them claim "I am person X". For example, a person may use his or her facial image to help them make the claim. A process then takes place to compare their facial image with a previously taken facial image of theirs. If the facial images match then the claim is successful. If the facial images do not match then the claim is unsuccessful. This process is also referred to as 1-to-1 or 1:1 matching, or authentication.

The development of biometrics has closely followed Moore's Law and the increasing capability of computer system in terms of processing speed, storage and bandwidth. This has led to an increase in the sophistication of pattern matching algorithms and a decrease in the cost of sensors. Cheaper sensors means they are able to be and increasingly becoming embedded in consumer devices, such as mobile phones.

The change in technology capability has occurred at the same time as identity related business drivers have gained prominence, such as the significant increase in e-commerce fraud and identity theft. These elements mean biometrics are appearing across a wide variety of applications that require user identification or verification.

2.2 Key Processes

The following are the key processes applicable to biometric solutions.

2.2.1 Enrolment

Enrolment is the process in which biometric information is collected, quality assessed, processed and stored.

Figure 1: Simplified Enrolment Process

As stated above, biometrics is the measurement of physical characteristics of an individual. The measurement is expressed in computer system as data. A biometric template, or profile, is a statistical analysis of the measurement, resulting in a specific reduced data set that can be used to represent the physical characteristics or features of an individual. It is important to emphasise that, for example, a fingerprint template is not the same as a fingerprint.

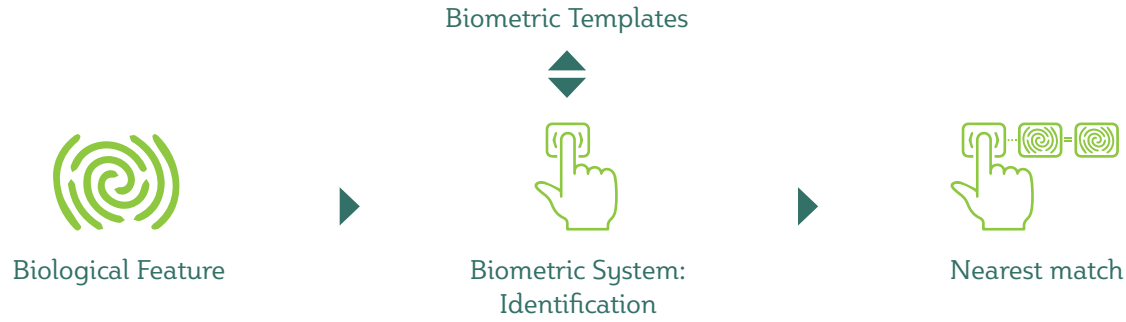
In the enrolment process, the data associated with the physical characteristic is collected (acquired) and, after a quality assessment, is processed in a specific way to create a template. The template can then be stored. Templates are specific to the type of biometric, and each biometric (fingerprint, iris etc.) has its own template.

The template generated during enrolment can subsequently be used for identification or verification. The template may be stored in a database of templates for all users, or may be store on a secure device or token specific to the individual, such as a smart card. The storage location affects the types of processes and services that can be supported by the system. If a single individual's biometric template is stored on a personal device at enrolment, the system can only support a verification process.

2.2.2 Identification

Identification is a 1:N matching process, comparing a newly collected template against a database of all templates for users of the system.

Figure 2: Simplified Identification Process



Typically, the database of biometric templates is stored on a server, remotely accessed over a network. This allows for identification checks from multiple interfaces against up to date information.

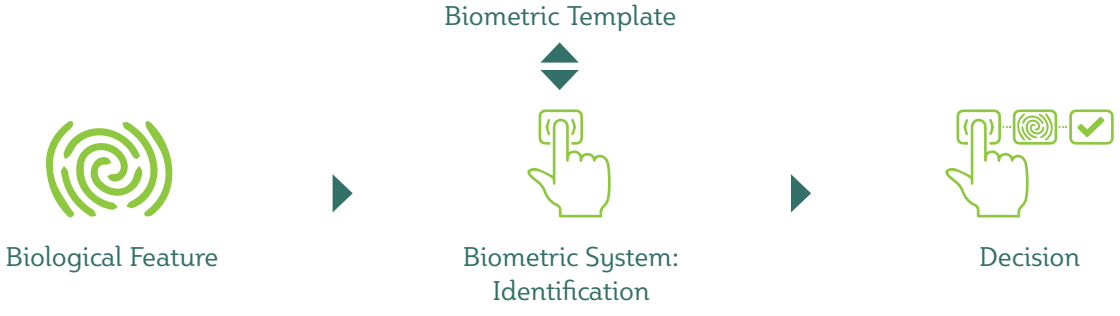
While a central database can be desirable as a single source of data, population scale databases can be difficult and expensive to manage and secure. For example, large database systems with lots of applications using it tend to have a significant number of operators accessing the data.

Access control policies can be difficult to implement and police, and may lead to unintended data leakage.

2.2.3 Verification

Verification is a 1:1 matching process comparing a newly collected template against a single template stored on an individual's device or security token, or alternatively against a single template stored with a customer record on a host system server.

Figure 3: Simplified Verification Process



Typically, for verification the biometric template is either stored in a database on a server or on an individual's secure device, depending on the type of biometric and the requirements of the service. For example, a voice biometric template may be stored on a server and be verified using any telephone, while a fingerprint biometric enrolled using a user's mobile phone is stored in secure hardware on the mobile phone and verified locally.

2.2.4 Accuracy

A biometric system needs to have an acceptable level of accuracy that can be defined in an unambiguous manner. As introduced above, a biometric template is only a statistical representation of a physical feature, not the feature itself; so a fingerprint template is not a fingerprint. By its nature, a statistical system is not 100% accurate and deviations from the idea occur.

The accuracy of the biometric solution is measured by three metrics: Failure to enrol rate, False Rejection rate and False Acceptance rate. These are described below. Although the accuracy issues described may represent a small proportion, when scaled to a population accuracy issues can affect a great many people.

2.2.4.1 Failure to Enrol

Failure to Enrol is the percentage of people who fail to be enrolled successfully into a biometric system. This is specified as the Failure to Enrol Rate or FTE as a percentage.

A notable failure to enrol problem is associated with fingerprint biometrics, because a percentage of the population have unusable fingerprints for measurement due to imperfections, wear, or being an amputee. This is particularly an issue with a population in a dry, dusty environment, manual labourers (including farmers), smokers and the older members of society.

2.2.4.2 False Rejections

False Rejection is defined as the percentage of verifications in which an incorrect verification or false rejection occurs – that is, people whose attempt to verify themselves fails even though they are in fact the registered person. This is expressed as a percentage for a False Rejection Rate or FRR. For example, if the FRR is 0.1%, it means that on average, out of every 1000 persons attempting to access the system, one will not be recognised by that system.

It is important to note that the occurrence of an instance of false rejection may result in denial of service to a valid user.

2.2.4.3 False Acceptance

False Acceptance is defined as the percentage of verifications in which an incorrect or false acceptance occurs. This is specified as False Acceptance Rate or FAR, and can be expressed as a percentage. For example, if the FAR is 0.01 percent, it means that on the average, one out of every 10,000 impostors attempting to breach the system will be successful.

It is important to note that the occurrence of an instance of false acceptance may result in access to a service being granted to the wrong person, in impersonation of another person.

2.2.4.4 Service Requirements for Accuracy

For any biometric technique there is a direct relationship between the failure rates for false rejection and false acceptance – that is, decreasing one rate increases the other. This means that for a specific service a trade-off must be made between the settings for FRR and FAR. The trade off made will depend on the application; for example, in financial services, it may be most important for rejections to be low, while in a government identity scheme the opposite may be true.

This trade-off is a decision that the organisation deploying the service elements must take. If a service is relying on someone else's biometric readers (for example, fingerprint readers built into mobile phone handsets) then the service may not be able to decide on the balance between failure rates and may have to adjust their policies to accept the reader owner's selection.

2.3 Key Requirements of Biometric Systems

2.3.1 Scalability

A key consideration is what happens to biometric system performance as the number of users increase, particularly to population scale.

The degree of uniqueness of the biometric affects the performance, particularly for identification functions. An ideal biometric would be able to uniquely identify each person in a large population, so that a service checking the database for a person's biometric template would return the unique identity for that person. However, since biometric systems use a statistical approach, the ideal is not possible from a single biometric and identification systems may need to use multiple biometrics in order to achieve this.

Scalability can also be important for verification. Verification is a 1:1 match between the biometric template acquired at time of verification against an individual's template, stored at time of registration/enrolment. The template may be stored centrally on a database server or may be stored locally on a secure hardware token.

For large populations, a key consideration is the time and costs required in order to enrol people with the appropriate level of quality.

2.3.2 Transaction Times

Depending on the application, the time required for a verification transaction may well be important. For example, it will determine how long or short a queue of people waiting to use the system will be. Enrolment processes do not normally have the same time constraints. Factors that influence transaction times can include:

- The selection of hardware and sensor for the application and the efficiency of the application software;
- The speed of the network if the solution is required to access a central database;
- The familiarity of the user with the system, how intuitive it is and how much training is required;
- The type of other authentication factors used with the biometric;
- Whether the process is supervised or not;
- Fallback (alternatives) in the event of failure in the biometric process or systems.

The requirements for transaction times vary considerably across different scenarios where financial services and payment applications may be used. When using a biometric for access control to logon to an online banking service, for example, the time taken to verify the biometric is not a significant constraint; a few seconds is fine. However, for in-store and in particular for transit payments a biometric verification may need to be completed with sub-second performance.

The requirements for each service scenario may mean that a particular biometric is appropriate in some situations and not in others. This may create weaknesses in overall service controls that can be exploited by attackers to subvert systems. Effective design and clear communication with users are key to maintaining effective security across all authentication methods.

2.3.3 Availability

If the biometric solution relies on access to a central database, the reliability of communications will have a direct bearing on the availability of services. Data communications services, whilst improving, continue to present challenges, with coverage – particularly in rural areas – often being poor. This is a particular issue in many emerging economies. Even in urban areas with apparently good coverage, insufficient investment in telecommunications infrastructure often results in capacity problems, so that a data connection may appear straightforward, but the connection is unreliable or has such a low data rate that it is unusable. These problems can affect both enrolment and subsequent identification or verification processes. And rural areas often have the bigger problem of no data coverage at all, even where there is mobile phone voice call coverage.

Financial services that provide access to account information held on central databases require good communications. Similarly, mobile money payments are online-only, meaning that connectivity is required to operator servers to process the transaction in real-time. However, other payments, such as payments with credit cards, can be designed to work offline in environments where communications is not always available or reliable. The selection of biometric verification method needs to be appropriate to the target service.

2.3.4 Verification Strength

The strength of verification depends on the use of a combination of different authentication factors. There are three types of authentication factors:

Two-factor authentication is stronger from a security point of view than single factor authentication, as users need to authenticate themselves with extra credentials. Two-factor authentication requires any two of the factors listed above. Integrating these factors into a single solution depends on the application.

Financial service and payment applications require strong authentication for effective risk management.

This is increasingly being recognised by regulators. In the forthcoming European PSD2 regulations, strong, multi-factor authentication is a requirement for all payment transactions covered by the regulations.

2.3.5 Environmental Factors

As introduced in the next section, different biometric techniques have different sensor requirements. Some sensors require a contact with a person to read the biometric, others are no contact is required. A biometric sensor that requires contact may have the potential to spread infections/disease, and so non-contact or easily cleaned alternative devices might be better. For example, fingerprint or finger vein devices, which tend to involve contact with a subject's finger, may not be suitable for use in an ebola area. Therefore, for some applications it may be important that the environment into which a solution is deployed is considered.

2.4 Standardisation and Interoperability

Outside of internationally agreed government identity schemes (most notably face recognition for e-passports) standardisation and interoperability for biometrics remains very limited. This is especially true for financial services and payments.

The lack of wide agreement has resulted in an abstracted, layered approach being adopted by standardisation initiatives for services rely on authentication. Where standardisation has been attempted, the interface to the biometric components of systems is separated from the interface to the authentication services.

This is the approach taken by international card schemes within EMVCo, the industry organisation responsible for payment standards. When a biometric is used for customer verification on a mobile handset, it is treated as any other consumer device cardholder verification method (CDCVM) and all the application knows was that the method passed or failed. In the FIDO Alliance , the online industry is taking a similar approach, where the detail of the verification biometric is separated from the protocol carrying the verification result.

The upshot of this is that there is little standardisation and interoperability in financial services and payments for biometric accuracy and security for enrolment, identification or verification functions. Organisations rely on services on an 'as is' basis, meaning that trust is not constructively propagated. This is a pragmatic approach to a lack of industry agreement.

3. Biometric Technology Options

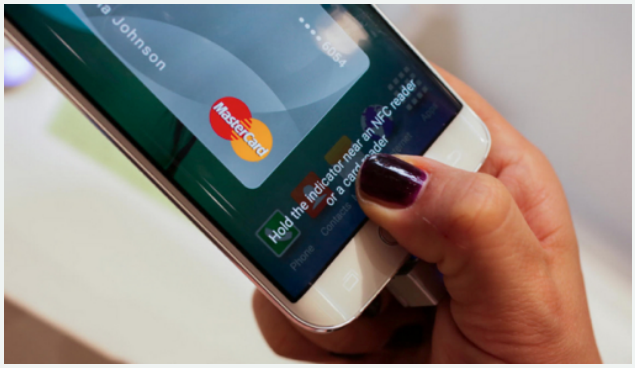
This section introduces the most common types of biometrics used in financial service and payment applications.

3.1 Fingerprint

Fingerprint technology is the acquisition of a fingerprint image and storage of the biometric template for the fingerprint. The main components in fingerprint technology are the sensors for acquiring the fingerprint, and the software that converts the fingerprint image into a fingerprint biometric template. Different types of sensors are available (for example, optical, ultrasound). Sensors are built into a wide range of devices from standalone terminals to mobile phone handsets.

Advantages	Disadvantages
+ Sensors are ubiquitous and cheap.	− Small percentage of population cannot enrol due to various issues with fingers.
+ Templates are small.	− Enrolment times vary depending upon characteristics of a person's skin and upon how many fingers are being acquired.
+ Fast to verify.	− Dirt or imperfections on fingers means that the verification performance can be impacted.
+ Unless the finger is damaged the fingerprint pattern does not change over time.	− Fingerprints may degrade and become less readable over time.
+ Fingerprints from multiple fingers can be used to improve accuracy.	

Figure 4: Fingerprint Recognition on Mobile for Samsung Pay[10]



Although fingerprints have been tried as a replacement to PINs for in-store POS payments in specific markets[11], the approach has not been deployed in significant numbers. The lack of interest from the card issuing banks seems to be due to the cost and complexity of managing the lifecycle of biometrics, in comparison with PIN. There has also been a lack of direction from the international card schemes who are responsible for policy and standardisation.

Fingerprint sensors are starting to be commonplace in high-end mobile devices and are being used for access control and payments. This was not the case 5 years or so ago, as Cellular News reported, when in 2009 only 10% of mobile phones in Japan were equipped with fingerprint sensors with no other market having any meaningful penetration. Following Apple's inclusion of AuthenTec technology in iPhones, service providers started to use Apple's fingerprint on handset services through Touch ID for service logon without passwords. Samsung and other device manufacturers have followed Apple's lead. Banks in many markets now allow customers to access account services by registering their device and enabling fingerprint verification as an authentication factor.

[10] http://cdn.bgr.com/2015/03/samsung-galaxy-s6-edge-samsung-pay-demo.jpg?w=624
[11] Such as the closed Pay-By-Touch service, https://en.wikipedia.org/wiki/Pay_By_Touch

In this case, verifying the identity of mobile phone itself, via the app, is one of the factors for strong authentication.

Most recently handset manufacturers, in particular Apple and Samsung, have enabled payment from payment cards stored on the device in secure hardware. For in-store payments, this requires the store's payment terminal to be enabled for contactless card payments. For remote payments, the card's details can be used from an app on the handset.

Instead of a PIN, the cardholder authenticates using the fingerprint reader on the handset prior to the transaction being provided to the merchant for submission to the payment networks for authorisation. To improve the user experience, the handset fingerprint readers are tuned to have a low rate of false rejections, and as such are not very secure[12]. Security is maintained through strong device authentication and risk management in the payment network, rather than relying solely on the biometric.

Face recognition refers to an automated or semi-automated process of matching facial images. The image of the face is captured using a camera and then processed in order to obtain a biometric template. Different algorithms can be used and various proprietary solutions are available from vendors. The sensors are digital cameras and can include video, 3D or infra-red facial scans. Sensors are available in many devices, such as mobile phones and proprietary device built for the purpose.

3.2 Face

Face recognition refers to an automated or semi-automated process of matching facial images. The image of the face is captured using a camera and then processed in order to obtain a biometric template. Different algorithms can be used and various proprietary solutions are available from vendors. The sensors are digital cameras and can include video, 3D or infra-red facial scans. Sensors are available in many devices, such as mobile phones and proprietary device built for the purpose.

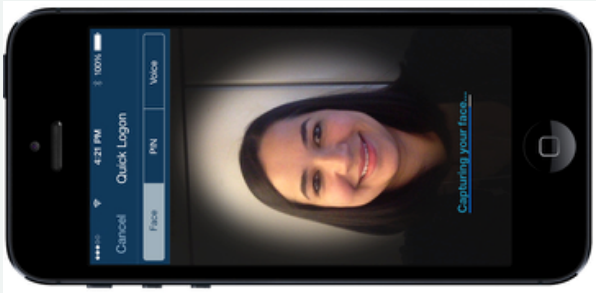
Advantages

+ No failure-to-enrol rate for a facial biometric.
+ Sensors are ubiquitous and cheap.
+ With 3D or motion capture, spoofing can be made difficult and costly to achieve.

Disadvantages

– Accuracy can be affected by the quality of the ambient lighting.
– Accuracy can be affected by the user wearing glasses.
– May be affected by facial feature changes over time.

Figure 5: Facial Recognition on Mobile for USAA[13]



According to American Banker[14], in 2015, financial services company USAA in the US rolled out facial recognition technology "across its entire membership base that lets them access its mobile app with a tap of their smartphone camera and a blink when prompted (to prove they're a live person and not a photo)." The mobile software and services is provided by Daon[15]. Since the success of this, a number of banks and financial services companies have stated their support for mobile facial recognition, notably the global card scheme MasterCard[16].

[12] http://www.biometricupdate.com/201602/vkansee-demonstrates-fingerprint-spoofing-with-clay-mold-at-mwc
[13] http://www.americanbanker.com/news/bank-technology/biometric-tipping-point-usaa-deploys-face-voice-recognition-1072509-1.html
[14] http://www.chyp.com/biometrics-are-already-mass-market-for-banking/
[15] http://www.daon.com
[16] http://www.cbc.ca/news/business/mastercard-selfie-pay-1.3459740

3.3 Finger Vein

Finger vein biometrics use the patterns of veins, vascular pattern recognition (VPR), or vein pattern recognition, in a person's finger to generate a template. The vein pattern is believed to be unique. Sensors use LEDs to light the subject, with the image captured by an appropriate CDD camera. Software translates the image into a biometric for matching purposes.

Advantages	Disadvantages
+ Good accuracy.	− Sensors not widely available.
+ Vein patterns are difficult to recreate / forge as blood needs to flow to register an image.	− Sensor cost significant in comparison to fingerprint, in part due to low adoption rates.

Figure 6: Finger Vein Verification for Online Banking in UK[17]

In financial services applications, finger vein recognition is used for access control to online banking and to ATM functions. In Japan, around 75% of banks are reported[18] to be implementing finger vein or palm vein (see the next section) biometrics in ATMs. The stimulus for the use of biometrics at ATMs in Japan was regulatory. In the mid 2000s, the Japanese regulator changed liability rules such that banks became liable for fraudulent withdrawals using stolen or counterfeit cards. Vein pattern recognition was used for customer ease of enrolment, as the failure to enrol rate is significantly better than fingerprint recognition technologies, and the cost of the reader was not prohibitive relative to the cost of an ATM. Deployments are happening in other markets, such as Turkey and Brazil, but do not appear to be on the scale of the Japanese deployment.

Finger vein verification is slowly expanding into other access control market, most notably an authentication factor for online banking. Barclays in the UK has issued PC finger vein readers to corporate customers to improve ease of use compared to a previous smart card and password based system.

A recent interesting approach to in-store payments used finger vein directly at the physical POS terminal. Natural Security[19] piloted a system with French banks and retailers where a finger vein reader was installed at the POS. The user's finger vein biometric template was stored on a bank card at enrolment. To use the card, it was inserted in a sleeve with a local area wireless interface. When the user approaches the check-out, the POS connects with the sleeve and the card. When the total amount is rung up, the user inserts their finger into the reader, the template is sent to the card and the card checks the stored finger vein biometric template against the one supplied by the terminal. This approach removes the need for a card insertion or a tap on the POS reader, and removes the need for a PIN, thereby speeding up the whole process.

While the accuracy performance of finger vein is superior to fingerprints, the cost of the technology appears to be a barrier to wider deployment, and there is little evidence that readers are being incorporated into mobile consumer devices or payment terminals.

[17] http://www.biometricupdate.com/wp-content/uploads/2014/09/barclays-finger-biometric-reader.jpg
[18] http://www.atm-security.co.uk/products/biometrics-in-an-atm.htm
[19] http://naturalsecurityalliance.org

3.4 Palm Vein

As per finger vein, palm vein scanners capture the hand's vein pattern using near-infrared light. Sensors are able to capture the palm image regardless of the position and movement of the palm. Software then translates the vein pattern into a template which can be matched for verification.

Advantages	Disadvantages
+ Good accuracy.	− Requires specialised sensors not widely available.
+ Vein patterns are difficult to recreate / forge as blood needs to flow to register an image.	− Cannot have anything on the hand that obscures infra-red e.g. glove, bandage etc.
+ No contact between subject and sensor.	

Figure 7: ATM using Palm Vein Readers in Japan[20]

As a non-contact device, palm vein readers are widely deployed for physical access control. They are less widely deployed for financial services, but have gained some traction in the ATM marketplace, particularly in Japan[21]. Initial deployments used palm vein as one factor in combination with a bank card as a second to provide secure access control to ATM functions.

The latest version allows access without a companion card. The manufacturer Fujitsu claims this can be achieved because the vein pattern in palms is particularly complex. The approach is for a user community of a bank. Research for this report did not find evidence that the approach is or is not suitable for national population-scale identification.

3.5 Iris

The pattern in the human iris can be measured and used for biometric identification or verification. Iris patterns are believed to be both highly complex and unique. Iris recognition systems are designed to cope with the fact that the scanning process is slightly variable, so two scans of the same eye will be slightly different. The degree of variation gives a measure of the probability that the subject is a different person. Sensors capture an image of the iris taken under near-infrared illumination.

Advantages	Disadvantages
+ High accuracy works well for identification applications.	− Enrolment requires reasonably controlled and cooperative user interaction.
+ 'Liveness detection' can be built in as an eye is never completely at rest22.	− Solution cost.

[20] http://www.digitalworldtokyo.com/entryimages/2006/04/Fujitsu_Palm.jpg
[21] http://www.fujitsu.com/global/about/resources/news/press-releases/2012/0926-01.html
[22] https://en.wikipedia.org/wiki/Saccade

Iris has had limited application in financial services applications. NTT DoCoMo incorporated a version of iris recognition linked to a payment system in a mobile handset in Japan in 2015[23], using a near infra-red LED to illuminate the iris and a camera to capture the image. There is no evidence of more widespread adoption. Iris recognition has been available for incorporation into ATMs for a number of years[24], but has yet to be deployed in any numbers.

3.6 Voice

Voice recognition compares a spoken word or phrase against a stored sample of the speech of the user. Voice recognition should not be confused with speech recognition, which is the ability to take action based on the words spoken. Voice biometrics works by digitising a profile of a person's speech to produce a stored model voice template. This uses perhaps the simplest and most ubiquitous of all the biometric sensors: the microphone. Microphones can be and are embedded in multiple form factors.

Advantages	Disadvantages
+ Very low cost.	– Prone to background noise and distortion.
+ Users are familiar with speaking.	– Factors such as a cold can change the characteristics of a user's voice.
+ The longer the subject talks, the more accurate the verification or identification. A minimum of five seconds.	– Slow verification for some applications.

In financial services, voice recognition is mainly used for access control to services rather than payments. For example, a number of the major UK banks (such as HSBC[25] and Barclays[26]) enable access to accounts using voice recognition as an authentication factor.

Voice has been less successful as a verification factor for retail payments. Over the last few years, several organisations have attempted and failed to bring voice payments to market. A relatively poor user experience for payments, relative to existing methods, potential lack of confidentiality in public spaces and poor transaction speed, seem to be the reasons why customers have not taken to the approach.

[23] http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0525-01.html
[24] http://www.atmmarketplace.com/news/diebold-launches-iris-recognition-atm/
[25] http://www.bbc.co.uk/news/business-35609833
[26] https://wealth.barclays.com/en_gb/home/international-banking/insight-research/manage-your-money/banking-on-the-power-of-speech.html

4. Biometrics In Financial Services Applications

This section considers current approaches for the use of biometrics in financial services applications, with particular focus on a successful user experience. As introduced above, typically, biometrics are used for access to services, for payment transactions as part of user authentication and, where specific requirements exist, to identify the individual user in within the complete user population.

4.1 Access to Services

Until relatively recently, when fingerprint sensors became available on high-end mobile phones, probably, the most used application for biometrics in conventional financial services was access control at Japanese ATMs. User verification is done using finger or palm biometric in conjunction with a bank issued card for strong two factor authentication.

For enrolment, the user needs to be an existing customer with a bank card, and typically uses a in branch kiosk to register their biometric and associate it to their account. User authentication includes the use of the bank card and personal identification number (PIN).

The finger or palm vein biometric is used instead of a PIN for higher value withdrawals. The driver for this was a change in regulation to make banks liable for ATM fraud.

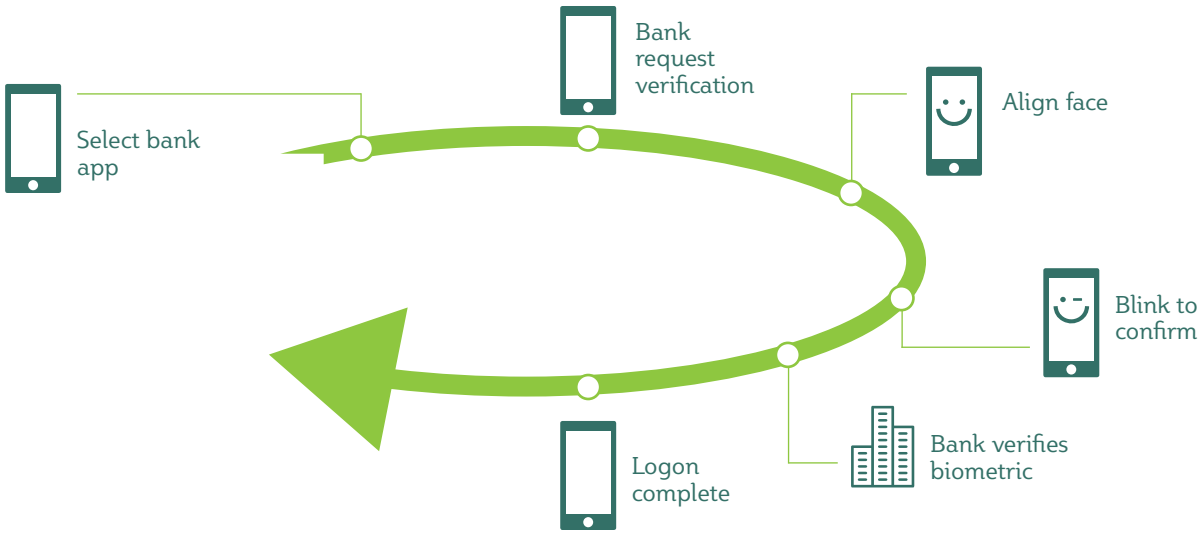
As well as ATMs, the other key digital access point for customers to financial service providers is the online services through the personal computer (PC) or mobile internet channel. Banks use many ways of authenticating customers for online banking. One of the most common, and simplest from an implementation point of view, is the use of multiple passwords with a '1 from n' entry for secondary passwords. Password based authentication is often inconvenient for users and are increasingly subject to fraud.

In response stronger authentication is starting to be mandated by regulators for online services. A more secure approach use a specific security token, different channel or smart card reader to receive or generate a one-time code to replace the secondary password. This two factor approach to authentication is often required for higher risk actions, such as adding a new payee to the list recognised for immediate bank transfer. Biometrics are being viewed as another one of the additional factors, and with the widespread penetration of mobile devices adding security without compromising ease of use.

One of the more interesting approaches on mobile uses face recognition. Enrolment here uses a bank app on a registered mobile device to capture and store the face biometric template at the bank host system. The bank relies on the mobile device registration and in app security to protect the integrity and confidentiality of the biometric.

The reason banks are using face recognition is for ease of use, convenient verification that customers seem to like. When logging on to a service, the user takes a 'selfie' and blinks for 'liveness detection'. The bank USAA were one of the first to use the approach and reported particular traction for younger, who are familiar with taking a selfie, and older customers, who final the method more convenient than a PIN or password.

Figure 8: Typical Customer Experience for Online Bank Logon using Face Verification



The convenience of this approach means it is starting to be used for other financial services, notably for e-commerce payments.

4.2 Verification for Payments

Card payments for e-commerce can increase security by incorporating an authorisation step between the customer and the card issuer at the point card details are entered at a merchant. This is referred to as 3D Secure and is standardised across the international card schemes to allow merchants and payment processors to more easily process transactions for cards from different schemes.

The problem with this approach has been that the step to authorise with the card issuer has involved yet another password, specific to the card, for customers to remember. Adding another password is difficult for many customers and has resulted in significant drop-outs at the bank authorisation step.

Replacing the password with a mobile biometric may improve the usability of the bank authorisation step in 3D Secure and reduce the occurrences of incomplete purchases for merchants. A new version of the 3D Secure standard is being worked on by EMVCo, due later this year, which is expected simplify and clarify how authentication techniques, including biometric, are used.

Remote payment transactions on the internet, whether by a PC or a mobile, will increasingly include a biometric verification on a mobile device, using face recognition, voice or an on-device fingerprint, for higher risk transactions.

For payments in-store at a point of sale, exactly the same approach can be performed when network coverage is good (either via the mobile operator or in-store wifi network). This is effectively a remote payment in an in-store environment.

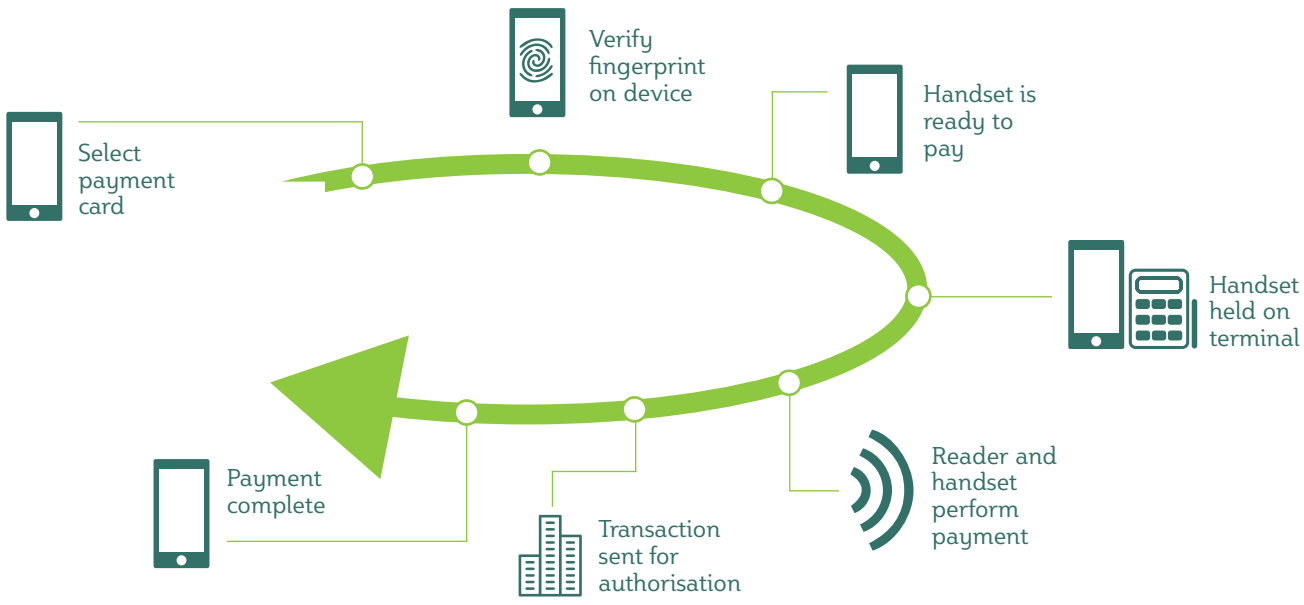
However, network coverage is often not available or reliable, especially in large merchants, transit operators or shopping malls. Here, conventional POS terminals are used for electronic payments. Increasing these come with contactless interfaces that allow local wireless connectivity to contactless cards and mobile handsets equipped with near field communications (NFC) interfaces. This allows card payments from mobile to be made using a local interface and on-device biometrics as an authentication factor.

Contactless card payments have transaction speed requirements that make the requirements for biometric verification more stringent than required for remote payments. When biometrics are used for these transactions, unlike the examples above, the biometric is stored and verified only on the handset itself. Currently, the only biometric used is fingerprint, on high-end smart phones device with appropriate sensors.

Enrolment uses the approach provided by handset operating system and the card issuer (i.e. a bank) has no involvement. The bank relies on the integrity and confidentiality of the handset operating system to control the biometric in a suitability secure way. No liability is accepted by the handset manufacturer. The security for the use of the biometric relies on the strength handset device authentication to bind the device to the customer.

The biometric is verified immediately prior to the payment transaction, when the mobile payment app on the handset calls the handset operating system to request verification. After successful fingerprint verification by the handset, the device is tapped on the POS terminal and a card transaction performed.

Figure 9: Typical Customer Experience for Mobile Contactless Payments using Fingerprint Verification



Multiple fingerprints can be stored on the handset. The user is responsible for managing access for fingerprint enrolment. It is quite common for other family members to register fingers to use a tablet or smart phone, and so any fingerprint check may not relate directly to the cardholder related to the bank payment app. This is recognised by the payment industry, and as such the consensus is that security is not as important as convenience.

Both of these methods could be reused for mobile money payments. The selection would depend on how in-store payments are supported. The first approach, to use a stored biometric at the card issuer (equivalent to the mobile money provider) requires good network access (which may be difficult to achieve reliably) but relatively low-end phones, while the second approach requirement the deployment of an appropriate POS terminal estate (which may be expensive) and NFC capable smart phones.

4.3 Identification in Financial Services

The above methods perform 1:1 biometric verification of the customer for the service in question, against a stored biometric template, using the customer identifier to point to the correct user data.

The use of 1:N biometric identification is less common in financial services. 1:N identification is particularly relevant when there is a requirement that individuals must not be duplicate users on the system. A typical example of where this is important is for government disbursements, such as for subsidies or welfare payments.

As discussed above, 1:N identification using needs accurate biometric method, or consideration manual interpretation is required, cross-referenced against other data sets, to identity the correct individual from a set of potential matches returned by the system. It is particularly important that the enrolment process is accurate and complete.

An example of a financial service identification system is the Nigerian Pension disbursement pilot. This is reported to have used fingerprint readers successfully reduce the occurrence of invalid payments and is rolling out throughout Lagos State[27].

Fingerprints are widely used for government identification schemes but, due to the high failure to enrol rates, can be difficult and expensive to operate. To overcome this problem multiple biometrics may need to be captured. In India, the national identity scheme, Aadhaar, captures a range of biometrics (ten fingerprints and two irises), to ensure uniqueness during enrolment and increase the chance that identification will be accurate over time. Once these are captured, an Aadhaar identity number is issued. To access services, users present their Aadhaar number, and that is used to access an online service (remotely) to check their biometrics for verification.

This is not an isolated case. A recent article in the Guardian newspaper reports[28] on the benefits and difficulties of biometric identification schemes for identity and disbursements in challenging environments. The report quotes the UNHCR as saying that "biometrics is not a panacea" and that it is "a tool amongst many".

Also in Nigeria, Consult Hyperion has used successfully the 'many tool' approach, taking a biometric as one method within a suite of functions to develop and run a pilot for agriculture subsidy disbursements to over 500,000 farmers[29]. As the farmers are in rural areas, without mobile network coverage in many cases, the system was designed to work offline as well as online. Field operatives captured a face image as a biometric, which was stored encrypted in the tablet and then, when the operative can back into network coverage, data was uploaded to a central database. Identification checking could then be done, on both the individual's documentation (if it existed) and image evidence, to ensure the farmer is only ever registered once. Verification for the subsidy disbursement is done at a merchant using a card issued to the farmer on enrolment.

Without accurate biometric technology, 1:N identification relies on the enrolment process itself. As the enrolment processes are often required to be manual to link identity documentation to an accurate set of biometric templates, the costs can be prohibitively high for financial services applications. As such, most biometrics in banking and payments are used for verification functions.

[27] http://www.vanguardngr.com/2016/02/n6-5bn-allocation-lagos-begins-biometric-verification-of-pensioners/
[28] http://www.theguardian.com/global-development-professionals-network/2016/feb/22/biometrics-aid-development-panacea-technology
[29] http://www.chyp.com/token-administration-platform-tap-e-goods-delivery/

5. Conclusion

This report aims to provide an overview of biometrics and their applicability for and use in financial services and payment applications. The focus of the report is on customer facing services, such as self-service account management and retail payments.

A biometric is a representation of a characteristic of a person, such as fingerprints, voice, face, or iris patterns. A biometric can be used (usually as one of a number of factors) for two functions:

Identification
– helping to answer the question"Who is this person?"

Verification
– helping the user to claim "I am person X".

Due to the cost and complexity of achieving very accurate biometrics at a population scale, financial services organisations are unlikely to rely heavily on biometrics for identification. Organisations will continue to rely on third party identification to meet customer due diligence requirements, in most applications.

In some applications, such as those supporting government disbursements, identification is a required feature of the system, in order to validate that an individual has only one account on the system. Biometric can be used alongside documentation evidence (where available) to help reduce multiple registrations. Due to the number of failures on enrolment, fingerprints are not necessarily the best biometric to use for identification and others types should be investigated.

For commercial financial services, biometric technologies have more applicability and are increasingly used for customer verification than for identification. Once a customer is identified to a service, a service user can enrol a biometric allowing the service to use it to link the user to the customer account.

Biometric technology aims to achieve a balance between security, convenience and transaction speed for a range of applications. Customers require low cost, convenient and reliable verification methods, using an approach that offers appropriate speed for the transaction being performed. Banks require straightforward systems for low cost enrolment and lifecycle management, using a biometric that offers a level of security appropriate to the action being undertaken.

Different technologies and different solution architectures address these in different ways. Corporate applications have been deployed using finger vein biometric readers for access control to internet business banking. For the mass market, mobile phones, in particular smart phones, are the platform of choice allowing voice, face or fingerprint recognition to be used, depending on the capabilities of the user's device and the environment in which the service is used.

Increasingly there is a role for biometrics within financial services account servicing and payments. Biometrics is used as one among several factors, to ensure strong authentication is achieved across different customer touch-points. For many mass market schemes, the catalyst has been the widespread penetration of mobile smart phones that allow apps to support multiple biometric methods; from voice and face recognition on lower-end devices, to fingerprint verification at the higher-end.

Using a mobile as a customer terminal means, banks and other financial service providers will be relying on the security of the handset technology for integrity and confidentiality of the customer biometric data. Providers need to recognise this and ensure that a biometric is one component of the solution that achieves secure authentication.

Table 1: Current Suitability of Biometric Methods to Financial Services and Payments

Biometric	Suitability for Mass Market Applications	Online Account Services Access	ATM Access	Remote Payments	In-store POS Payments
Finger-print	Low cost, wide deployment, difficult enrolment, low accuracy	Fingerprint capable mobile	Pre-checked on fingerprint capable mobile	Fingerprint capable mobiles	Pre-checked on fingerprint capable mobiles
Face	Low cost, wide deployment, easy enrolment, low accuracy	Mobile camera phone	May be suitable if infra-red used.	Mobile camera phone	Pre-checked on mobile camera phone
Finger vein	Limited deployment, easy enrolment, high accuracy	With PC Reader	With Reader	With Reader	With Reader in Terminal
Palm vein	Limited deployment, easy enrolment, high accuracy	With PC Reader	With Reader	With Reader	With Reader in Terminal
Iris	Very limited deployment, difficult enrolment, high accuracy	Not suitable	Trialled. Currently not suitable	Not suitable	Not suitable
Voice	Low cost, easy enrolment, low accuracy	Any mobile or fixed line telephone	Not suitable	Any mobile or fixed line telephone	Not suitable

About Consult Hyperion

Consult Hyperion (www.chyp.com) is an independent IT company that specializes in using considered best practice from within industrialized economies to deliver transformational products and services in emerging economies. Our focus is on the design of intuitive secure transparent Digital Financial Services (DFS) which require minimal staff training, promote self-sufficiency within the local market and can be scaled nationwide. Our successes include M-PESA in Kenya and the GES TAP eVoucher delivery system in Nigeria.

Formed in 1984, Consult Hyperion's core business is the design and implementation of new retail payment services, primarily for the international payment schemes American Express, Mastercard Worldwide and Visa Inc. as well as the domestic payment schemers in Australia, Canada, Scandinavia and the USA. Our clients range from the global payment brands to national governments via local regulators, international and local banks, non-banking financial companies (NBFCs), MFIs, telecoms operators, NGOs, donor agencies and their suppliers, across the globe. The products and services we have helped to design and deliver are used by hundreds of millions of people across every continent, every day. There will be at least one in your wallet or phone.

About FSD Africa

FSD Africa is a non-profit company which aims to increase prosperity, create jobs and reduce poverty by bringing about a transformation in financial markets in Sub-Saharan Africa (SSA) and in the economies, they serve. It provides know-how and capital to champions of change whose ideas, influence and actions will make finance more useful to African businesses and households. It is funded by the UK aid from the UK Government.

FSD Africa also provides technical and operational support to a family of ten financial market development agencies or 'FSDs' across sub-Saharan Africa called the FSD Network.

About the FSD Network

The FSD Network is an alliance of organisations or 'FSDs' that reduce poverty through financial sector development in sub-Saharan Africa.

Today, the FSD Network:

- Comprises two regional FSDs in South Africa (est. 2002) and Kenya (est. 2013) and eight national FSDs in Kenya (est. 2005), Ethiopia (est. 2013), Mozambique (est. 2014), Nigeria (est. 2007), Rwanda (est. 2010), Tanzania (est. 2005), Uganda (est. 2014) and Zambia (est. 2013)
- Is a leading proponent of the 'making markets work for the poor' approach
- Specialises in a number of themes from agriculture finance and savings groups to payments, SME finance and capital market development
- Represents a collective investment of $450+ million by DFID; Bill & Melinda Gates Foundation; SIDA; DANIDA; Foreign Affairs, KfW Development Bank; the MasterCard Foundation; RNE (Netherlands); Trade and Development Canada; and the World Bank
- Spends $55+ million per year, predominantly through grant instruments
- Employs over 130 full time members of staff and a uses wide range of consultants

fsdafrica

FSD Africa, Nairobi, Kenya
info@fsdafrica.org
@FSDAfrica

www.fsdafrica.org

consult hyperion
securing tomorrow's transactions

Consult Hyperion, 12 The Mount
Guildford, Surrey GU2 4HN
info@chyp.com
@chyppings

www.chyp.com

UKaid
from the British people

Department for International Development
enquiry@dfid.gov.uk
@DFID_UK

www.gov.uk