Smart Insights

Biometrics to secure and optimize payments

In collaboration with:

TRUSTECH
PAY | IDENTIFY | CONNECT & SECURE
Incorporating CARTES SECURE CONNEXIONS

WHITE PAPER

Table of Contents

Our market information (qualitative and quantitative) is based on a combination of primary and secondary research, along with our long-standing experience of the industry. Intelling takes no responsibility for any incorrect information supplied to us by manufacturers or users.

The information contained herein is general in nature and is not intended, and should not be construed, as professional advice or opinion provided to the user. This document does not purport to be a complete statement of the approaches or steps, which may vary according to individual factors and circumstances, necessary for a business to accomplish any particular business goal. This document is provided for informational purposes only; it is meant solely to provide helpful information to the user. This document is not a recommendation of any particular approach and should not be relied upon to address or solve any particular matter. The information provided herein is on an "as-is" basis. Amounts are converted according to recent conversion rates known at time of publishing. The converted amounts are only a gross evaluation and are not intended to reflect accurately the variations of currency rates.

Author: Giovanni Kague - gkague@smartinsights.net

Publication date: October 2017

Published by Intelling, 3 avenue Clot-Bey, 13008 Marseille, France

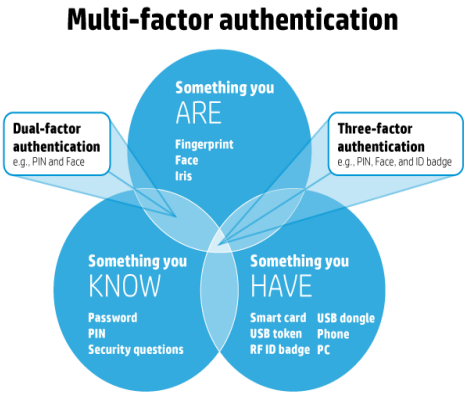
www.smartinsights.net-report@smartinsights.net

1. Biometrics for payments

New technological solutions are gradually being implemented to combat document fraud, identity theft, and cybercrime. Biometrics is one of these technologies that has quickly established itself as the most relevant means of identifying and authenticating individuals in a fast and reliable way, through the use of unique biological characteristics. Biometric payment is a Point of Sale (PoS), among others, technology that uses biometric authentication to identify the user and authorize the deduction of funds from a bank account.

Currently, numerous applications use this technology whereby in the past it was reserved for sensitive applications such as the security of military sites. Nevertheless, biometrics is now developing rapidly through applications in the public domain. Technological innovations like biometrics and mobile devices have extended the range of potential services. Biometrics and identity solutions companies, such as Idemia, Gemalto, G+D and others … help develop online banking and payment by providing state-of-the-art technologies for the entire digital chain, ranging from registration of customers and their devices (*e.g.* mobile, tablet), graduated multi-factor authentication (*e.g.* biometrics, mobile, smart card), to a digital vault that guarantees the long-term integrity, confidentiality and legal value of contracts and proof.

Often, systems use Multi-factor Authentication (MFA), in which the biometrics takes the place of the card swipe and the user types in a PIN (Personal Identification Number) as usual. MFA combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.



(Source: HP)

According to news media source, *letstalkppayments*, the global biometrics market is expected to see a substantial growth over the coming years. Some estimates suggest that by 2021, the market will reach a value of US$ 30 billion (EUR 26 billion), with its primary revenues shifting from the government sector to banking and consumer electronics.

2. Different types of biometrics

The different types of biometric identifiers include fingerprints, finger-vein, retina and iris patterns (eye), hand geometry, earlobe geometry, voice waves, DNA, facial recognition and the heartbeat.

According to *Visa's* 2016 study, fingerprint recognition was voted the most favorable biometric authentication method by consumers due to ease of use and security and a report from *Juniper Research* entitled "Top 10 disruptive technologies in fintech: 2016," listed biometrics as the number one technology to transform eCommerce.

Fiserv, an American provider of financial services technology, reported that fingerprints trump passwords in terms of security in the eyes of consumers: 41% of consumers stated they would feel secure using a password as an authentication method to confirm their identity when using a mobile app, compared to 62% for fingerprint technology, thus proving that this technology holds huge potential for the payment security market. For some time now companies such as Apple Pay, Android Pay and Square Cash, a peer-to-peer payment app, have been using fingerprints to add an extra layer of security to their payment processes for user peace of mind.

Fingerprint

Modern capacitive touch fingerprint sensors (such as the Touch ID sensor on the latest Apple iPhones and sensors on recent Android devices) recognize the fingerprint and unlock the device in less than a second, quicker than inputting an extensive password. The fingerprint is stored securely in the phone for other authentication processes, which also include payments through Apple Pay or Samsung Pay. One can therefore use their smartphone's home button as the fingerprint biometric sensor.

Facial recognition

In terms of facial recognition as methods for payments, MasterCard says it plans to bring "selfie pay" security checks to more than a dozen countries. In 2015, the company started trialing the technology, which uses facial recognition to authenticate users' identity, but now says it has firm plans to roll the feature out to users after positive reactions from testers.

> Samsung's deployment
>
> The Samsung Galaxy S8 has deployed facial recognition technology, an iris and fingerprint scanner, as well as Samsung pay to make authenticated payments.

To use the facial recognition payment authentication platform, selfie pay, customers will have to download MasterCard's app to their phone or tablet, then after entering their credit card information, as normally done during an online payment, they'll hold their device up to their face to take a quick picture. Users will have to blink to prove that they're not holding a photograph in front of the camera, and MasterCard says its algorithms can tell when someone is trying to fool the system by using a video.

Voice recognition

To use voice biometric for mobile payments, consumers complete a one-time voice registration process during which a few spoken words are used to generate a unique biometric voiceprint. Subsequently whenever a purchase is made, the user voice verifies the transaction over the phone. The voice biometric system works by analyzing 117 parameters of voice, filtering out any other noises. Since, theoretically, no two voices are the same, voice recognition is bound to become an alternative

for online credit card payments.

Finger-vein

Finger veins technology for biometric authentication uses near-infrared light that is transmitted through the finger. The infrared light irradiates the back of the hand and light passes through the finger. A camera located at the palm side of the hand captures the light. As hemoglobin in the blood absorbs the infrared light, the patterns of veins in the palm side of the finger are captured as shadows, therefore transmitting near-infrared light through a finger, being suitable for the acquisition of its vein pattern.

Finger-vein at the PoS

Nordic payments processor, NETS and UK biometric company Sthaler have trialed finger vein recognition at the PoS. Sthaler's FingoPay, works via an electronic reader, which builds a 3D map of the customer's finger veins, generating a 'natural personal key', thus removing the need for the individual to enter any personal details upon registration for payments.

3. Enrollment

No matter what biometric methodology is used during the enrollment process, the identification verification process remains the same. A record of a person's unique characteristic is captured and kept in a database. Later on, when identification verification is required, a new record is captured and compared with the previous record in the database. If the data in the new record matches that in the database record, the person's identity is confirmed.

Know your customer (KYC), a process of a business identifying and verifying the identity of its clients, prevent banks from being used, intentionally or unintentionally, by criminal elements for Money Laundering Activities (MLA). Implementing the KYC principle, banks have enrolled their customers in biometrics payments in order to decrease the likelihood of MLAs occurring in their business operations.

The enrollment process of Apple's Touch ID is an example of how major biometric mobile payment systems, including the Samsung Pay and Google Pay, operate. With an iPhone 6, iPhone 6 Plus or later, one can use Touch ID to make Apple Pay purchases in stores, within apps, and on websites in Safari web browser.

In order to enroll into Touch ID to make purchases, one would need to first create a passcode for the device as a process of multi-factor authentication, then register their fingerprints into the phone through a series of guided steps. After the registration, one can make a purchase by lightly touching the home button. After Touch ID is set up, it can also be used to unlock the Phone by just pressing the Home button using the finger registered with Touch ID.

Biometric cards are also deemed to take contactless payments to the next stage, according to security and identity solutions specialist *Idemia*. The way biometric card payments work is that the cardholder's biometric fingerprint template is securely stored in the chip of the card. As the card is inserted into/tapped onto an EMV payment terminal, cardholders place their finger onto the sensor and the deploying company's algorithm matches the fingerprint to the template stored in the card, replacing the manual entry of a PIN. The added security enables merchants to extend the threshold of contactless payments, which are currently capped at smaller amounts.

(Source: Gemalto.com)

India

With Aadhaar Payment, Indians can link their bank accounts to their fingerprints and pay traders equipped with a biometric reader for goods and services with a scan of their finger. A merchant only needs a smartphone, which is biometrically authenticated and consumers can enroll by imputing their bank name with the account number along with their Aadhaar number to facilitate payments. Since consumer fingerprints already exist in the Aadhaar database, the enrollment process only requires the consumer's knowledge of his/her bank credentials. Now, 1.3 billion Indians have registered their biometric data under the government's unique identification program, Aadhaar.

The cardholder's biometric data is enrolled at the Bank branch using either a secure tablet with the assistance of a teller or 24/7 with a kiosk. The fingerprint reference data is securely stored in the card's secure chip and is not kept on the Bank's servers nor sent over the air to a personalization bureau. The fingerprint sensor is large enough and well positioned enough on the card body to enable a seamless user experience: by holding the card pretty much as always before, the cardholder will perform biometrics verification with his/her enrolled finger.

4. Card payment at physical commerce

Multiple options are available at physical commerce.

Regular cards security can be enhanced when using fingerprint verification as an EMV user authentication method. In this case, fingerprints are read on the POS terminal, and then sent to the card. The card chip performs a "match on card" operation, comparing the proposed fingerprint with the one it has in a secure memory. The card remains responsible for the authentication process.

(Source: Ingenico)

Ingenico, a France-based company that provides technologies involved in secure electronic transactions, also launched its biometrics PoS terminal range, iWB Bio Series, mostly present in India. The biometrics PoS terminal uses the unique 4-Factor-Authentication where it combines Chip, Pin, fingerprint verification and GPS tracking, thus making it a secure mode of transaction while simultaneously building an efficient fraud management system.

With biometric cards, a simple card insertion (contact mode) or tap (contactless mode) on the POS will be sufficient to complete the transaction. PIN code can be used as a fall-back solution whenever the cardholder's fingerprint can't be used - like ATM cash withdrawals for example.

Germany

In Germany, a variety of Edeka's, the largest supermarket corporation that currently holds a market share of 26%, consumer markets and a few school cafeterias have implemented a payment system called digiPROOF, where the user's fingerprint is combined and encrypted with the unique device ID before it is sent to the authentication server called TrueMe (verification). This system can be used for online-payment, online-banking, online-broking and other password-protected web sites and services.

The companies that are operating in the realm of biometric payment cards are Idemia, a French multinational company; Gemalto, an international digital security company providing software applications, secure personal devices such as smart cards and tokens, and managed service, and others.

UK and US

UK's Thriftway and Kroger, both supermarket and food store, which uses a fingerprint payment technology. Another system is used by the supermarket/food store, where the biometric authentication is combined either with the telephone number or the date of birth. The San Francisco based supplier of this technology is Pay by Touch.

An alternative is to add a fingerprint sensor on the card itself. In this case, the user's fingerprint is read and compared on the card, with a "match-on-card" process. At the end of the operation, the card gives a standard response to the terminal to prove it has authenticated the user.

5. ATMs

Conventional authentication systems at the ATM, telephone banking and online banking as well as many other banking applications are vulnerable to fraud and can be secured through biometrics. ATM Industry Association (ATMIA), the global nonprofit trade association that services an industry built around the global growth of the ATM, launched a dedicated forum that will discuss how ATMs can better serve the under-banked and unbanked, to foster best practices and new ideas that go deeper than using ATMs to cash checks or withdraw cash securely from preloaded electronic benefit transfer cards and other products.

Japan

Japan-based Fujitsu launched a new range of ATM pilots on the European market, featuring PalmSecure biometric technology and support for mobile NFC. The ATM offers a technology that authenticates the user by reading the unique pattern of veins in the palm of the hand. The firm says the technology maximizes security levels when incorporating mobile applications, such as access to the ATM using contactless technology, or interacting with mobile devices via NFC.

Biometrics in banking security is beginning to be piloted by some ATM companies. Instead of merely having to insert the card and type in a PIN number, the new pilot machines use fingerprint, iris and

facial recognition technology that require the ATM card as well as a biometric scan before the individual can go through with the transaction. Biometrics are being implemented into ATMs in order to tackle ATM fraud such as:

- Skimming attacks: the most popular breach in ATM transaction, where a card swipe device reads the information on ATM card,
- Card trapping: placing a device directly over or into the ATM card reader slot.

With the deployment of biometrics in the ATM, there is an extra layer of security that these hacks are not designed for, which also allows consumers to be more aware when inserting their cards into the ATMs, knowing there will be biometric identification. Such fraudulent incidents can be minimized, as an added layer of authentication is introduced, which ensures that even with the correct pin information and in possession of another person's ATM card, the user's biometric features cannot easily be faked. Further advantages include:

Russia

Russia, Leto-bank, a subsidiary of Russia's VTB Bank, has ATMs equipped with fingerprint scanners to enable cardholders to withdraw cash without a card, but with PIN. Meanwhile, Sberbank of Russia also piloted biometric identification solutions, whereas holders of Sberbank-issued social cards are able to pay for products and services by having their fingerprints scanned.

- All attributes of the ATM cards being maintained,
- Reduced counterfeiting attempts due to enrolment process that verifies identity and captures biometrics.

These advantages are for the benefit of users as well as system administrators because the problems and costs associated with card lost, reissued or temporarily issued cards, can be avoided, thus saving some costs of the system management.

6. Mobile payments

According to *Visa*, with the likes of Apple's Touch ID making fingerprint recognition familiar, the technology is one of the most popular forms of biometrics for payments, backed by 53% over other methods. In contrast, just 23% prefer iris scanning, 15% facial recognition, 12% voice recognition and 10% behavioral biometrics. There is a slight preference for using biometrics in the real world over online: 48% want to use it for payments when on public transport, 47% in a bar or restaurant, 46% on the high street, 40% shopping online and 39% when downloading content.

Implementation benefit

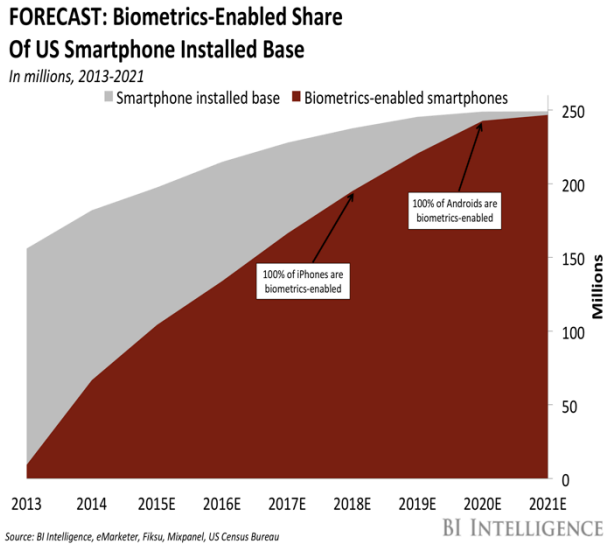
Infrastructure: Implementing mobile biometric payments will allow merchants to use the already existing smartphone infrastructure, such as the fingerprint scanner and camera on the new models of the IPhone and Samsung devices, in order to authenticate payments in a convenient and cost saving manner.

Mobile payments using biometrics to authenticate the user was forecasted to reach close to US$ 2 billion (EUR 1.7 billion) in 2017, up from US$ 600 million (EUR 523 million) in 2016, according to data from *Juniper Research*. The reason for this increase is attributed to the growing availability of fingerprint sensors on smartphones and tablets (60% of smartphones are expected to launch with fingerprint sensors in 2017). According to the research,

driving the movement to biometrics payments is Apple Pay, which paved the way for consumers to make payments in stores and on apps using fingerprints. Android Pay and Samsung Pay helped drive adoption further with their own biometrics capabilities, noted the report.

In addition to that, the growth of biometric payments is being helped by the growing availability of fingerprint sensors on smartphones and tablets.

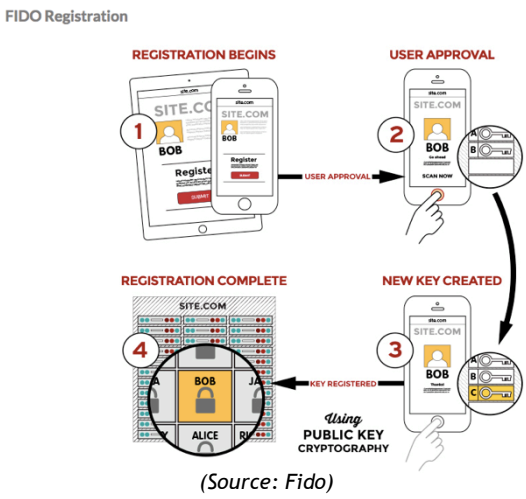
In a report from *BI Intelligence*, the market for biometrics-enabled smartphones in the US was sized and here are some key takeaways from the report:



- US smartphone makers are rapidly integrating biometrics-based features, such as fingerprint scanners, into their devices. BI Intelligence forecasts that 99% of installed smartphones in the US will be equipped with fingerprint scanners by 2021. The shift will happen much sooner for the installed base of iPhones in the US — nearly all of which will be biometrics-enabled by 2018.
- Biometric technology is moving beyond fingerprints. Right now, biometric verification is largely concentrated on fingerprint-scanning technology on mobile phones. But the technology is expanding, and other verification methods, including facial recognition and iris scanning, are becoming more popular.
- Although biometrics pose their own security challenges such as the risk of the permanent biological identifiers stored in databases and devices being very valuable to hackers, solutions to these security challenges include implementations from the Fast Identity Online (FIDO) Alliance formed in 2013 to revolutionize online authentication by developing open, interoperable industry standards that leverage proven public key cryptography for stronger security and device-based user verification for better usability.

The FIDO Alliance protocols work during registration with an online service, whereby the user's client device creates a new key pair (private key) to match against the public key. It retains the private key and registers the public key with the online service. Authentication is done by the client's device proving possession of the private key to the service by signing a challenge. The client's private keys can be used only after they are unlocked locally on the device by the user. The local unlock is accomplished by a user-friendly and secure action such as scanning a finger, entering a PIN, speaking into a microphone, or inserting a second-factor device.

The standard organizations driving the development of mobile biometric payments are the FIDO Alliance and EMVCo, who are working together to provide a new authentication standard for mobile wallet and payments developers, allowing consumers to use certified, on-device biometric verification when making in-store or in-app purchases. The work will be developed as an extension to



(Source: Fido)

the Web Authentication specification already in development by the World Wide Web Consortium (W3C), which offers authentication standards for web browsers and platforms.

In conjunction, the NFC Forum is the global organization with a charter to advance the use of NFC technology, playing a leading role in fostering the development of secure NFC solutions. The organization's primary role is to develop interface specifications that enable the use of NFC in the broadest range of applications, which have varied security needs, including those of biometric mobile payments.

The interface specifications consider that each mobile payment brand has its own business model, features, and benefits, some are the products of partnerships among device makers, payment processors, and banks, while others are built around a relationship between the payment provider and each merchant. Some use NFC in card emulation mode to perform transactions, while others use QR codes or a radio-equipped phone case. Some work with any credit card, while others are limited to specific brands. Some can work with existing magnetic stripe POS terminals, while others require newer-technology terminals or add-on dongles.

Advantages of NFC in mobile payments

- Global - based on industry standards and supported throughout the world,
- Proven - millions of people globally are already using NFC to pay for purchases, access public transit, and more,
- Popular with consumers - *NFC World*: 90% of consumers who have used NFC for mobile payments would use it again,
- Secure - strong authentication methods; device on/off switch for NFC; data encryption; proximity: NFC's short transmission rate.

7. Conclusion

The implementation of biometrics is a convenient and cost efficient way to further secure the payment process online, offline, and with the devices involved in the transaction. It also eliminates the risk of losing a card or mobile phone whereas biometric fingerprints (or Payment Fingers) will always be available to make a payment.

Of more than 14,000 people from across seven European countries quizzed by *Visa*, nearly three quarters see two-factor authentication, where a biometric is used in conjunction with a payment device, as a secure way to confirm an account holder. When asked about the benefits of biometric authentication, half of respondents say that it could create a faster and easier payment experience than traditional methods, while a third like the fact that the technology means that their details would be safe even if their device was lost or stolen. On the consumer side, this supports the notion that a majority of individuals consider biometric payment a safe and convenient way to pay online as well as offline, thus supporting the process' rapid growth.

Further developments in payments include Invisible payments, a term used to describe how the mechanics of payments will fade into the background and thus becomes more or less invisible, such as the removal of the card and handset from the payment process. Invisible payments are expected to be the next revolution in the payments industry. Since the creation of the payment card, only small innovations have occurred, such as contactless payments. Bankcards keep being the most successful and used electronic payment instrument, without any other instrument bringing strong competition to the market.

The Smart Insights Report "Invisible payments key to omni-channel commerce" conducts a detailed analysis of this emerging market segment. Looking to the payments industry as a whole, Smart Insights analyzes the main trends shaping the payments landscape in the last years, as well as retail. Focusing on the needs identified in the market, drivers and constraints for the implementation of invisible payment systems are presented, while highlighting the potential benefits for multiple stakeholders. To see more: http://tinyurl.com/zlkqtwl.

Glossary

ATMIA	ATM Industry Association
EMVCo	Europay, MasterCard, and Visa consortium
FFIEC	Federal Financial Institutions Examination Council
FIDO	Fast Identity Online
IoT	Internet of Things
KYC	Know Your Customers
MFA	Multi-factor Authentication
MLA	Money Laundering Activities
NFC	Near Field Communication
OTP	One-time Password
PIN	Personal Identification Number
PoS	Point of Sale
TSYS	Total System Services
W3C	World Wide Web Consortium

Published by:
Intelling, 3 avenue Clot-Bey, 13008 Marseille, France
www.smartinsights.net -report@smartinsights.net

Publication date: October 2017