GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Biometrics -
The Must-Have Tool for Payment Security

A White Paper from Goode Intelligence

www.goodeintelligence.com

First Edition October 2015

Published by:
Goode Intelligence
United Kingdom

www.goodeintelligence.com
info@goodeintelligence.com

CONTENTS

Payments are the major driving force for the wide-scale adoption of biometrics in the consumer market. Biometric systems are being adopted across a wide range of payment types with many different biometric technologies involved. This white paper from research and consultancy company Goode Intelligence (GI) explores the adoption of biometrics for payment security, drawing on recent published research on biometrics for payments.

PAYMENTS – THE DRIVING FORCE FOR CONSUMER BIOMETRIC ADOPTION

Payments are a major driving force for the wide-scale global adoption of biometrics in the consumer market. Today, millions of customers (350 million plus during 2015) are using biometrics on a daily basis around the world to provide secure convenient user authentication and transaction authorisation with this theme is set to continue with a forecast of over three billion biometric payment users by 2020.[1]

Over Three Billion Biometric Payment Users by 2020

Mobile payments, both in-app and in-retail store, have been a major contributor to the adoption of biometrics. The need for [authentication] speed twinned with the ability to include payment authentication to contactless payments has resulted in fingerprint biometrics becoming the standard for the latest mobile payment and mobile wallet solutions. Smart mobile device manufacturers, including Apple (Apple Pay) and Samsung (Samsung Pay), and mobile platform owners (Apple, Google and Microsoft) are using biometrics to win the war of owning payment delivery for in-store transactions.

Mobile payments are an important driving force for biometric adoption but mobile is not the only payment method that is embracing biometric technology. Goode Intelligence's research has discovered that other payment methods, from cash to Bitcoin, have developed biometric solutions in an attempt to reduce growing levels of payment fraud and to enable the adoption of alternative payment solutions.

Goode Intelligence White Paper

GI's white papers offer analyst insight from research extracted from primary sources including surveys, analyst reports, interviews and conferences.

GI Definitions

Apple Pay: Apple's mobile wallet solution

Samsung Pay: Samsung's mobile wallet solution

Bitcoin: An alternative payment solution using Blockchain technology

Blockchain: A distributed database or ledger that is used by Bitcoin

[1] Forecasts taken from "Biometrics for Payments – Payment Security Gets Personal; Market & Technology Analysis, Adoption Strategies and Forecasts 2015-2020" published by Goode Intelligence, October 2015: **http://www.goodeintelligence.com/report-store/view/biometrics-for-payments-payment-security-gets-personal-market-technology-analysis-adoption-strategies-forecasts-20152020**

BIOMETRICS – DELIVERING PAYMENT INNOVATION

There are a number of important trends currently happening in the world of payments that include:

- Rise in Mobile Payment and Wallet solutions
- Rise in Mobile Payment transactions
- The emergence of wearable payment solutions
- Steady reduction in use of cash for payments (although 48% of UK consumers still prefer cash to electronic)[2]
- Rise in Payment Fraud including:
    - Card-Not-Present (CNP) fraud especially with eCommerce payments
    - Fraud at the ATM
    - Card provisioning fraud for mobile payments
- The emergence of alternative payment solutions including Bitcoin

Against this backdrop, we are seeing the pressing need to improve payment security and the desire to replace cumbersome user authentication mechanisms with solutions that are both convenient and can reduce the risks of identity theft. This is where biometrics is meeting both the needs of improved security and supporting new methods in how we pay for goods and services.

Mobile Payments – Has Fingerprints Won?

The use of smartphones as a payment tool has been in the pipeline since the early years of this century. A mixture of business issues (who owns the wallet and the customer) and security challenges meant that there were few successful examples outside of NTT DOCOMO in Japan. Back in 2004, DOCOMO really established the framework for biometric mobile payments when the Japanese mobile network operator (MNO) launched the i-mode FeliCa™ (an RFID chip similar to NFC) smart wallet service enabling smartphones to act as contactless credit cards at POS terminals. DOCOMO launched a number of Fujitsu supplied smartphones, including the F901iC (see image in right-hand column), that came equipped with swipe fingerprint sensors supplied by AuthenTec. It allowed customers to use their smartphones to pay for goods in physical stores and authorise the payments with their fingerprints.

In 2012 Apple paid $356 million for AuthenTec and in September 2013 launched the iPhone 5S with the Touch ID fingerprint system.

A year later in October 2014, Apple launched Apple Pay in the USA enabling users with Touch ID and NFC enabled iPhones to use their phones to make payments in-store – 10 years after DOCOMO introduced biometric payments on smart mobile devices.

Apple Pay is probably the most successful contactless mobile payment

NFC: Near Field Communication is a set of protocols that enables devices to establish short-range radio communications with each other.

Touch ID: A fingerprint biometric solution implemented by Apple and available on the iPhone 5S, the iPhone 6, 6S, the iPhone 6 Plus, the iPhone 6s Plus, the iPad Air 2 and the iPad Mini 3.

[2] Cashless payments overtake the use of notes and coins. BBC, 21 May 2015: **http://www.bbc.co.uk/news/business-32778196**

solution to date and much of its success is down to the frictionless user authentication experience that Touch ID fingerprint solution provides. The biometric authentication solution has also enabled Apple to negotiate favourable transaction fees with the payment scheme providers and issuing banks.

Over 770 million Smart Mobile Devices with integrated fingerprint sensors by 2016

Goode Intelligence Forecasts[3]

Fingerprint biometrics dominates the current payment biometric market with 50 percent of total users. By 2020, Goode Intelligence predicts that other non-fingerprint biometric modalities will dominate with 72 percent of payment biometric users (fingerprint down to 28 percent).[4]

Non-fingerprint biometric modalities that are being primed for mobile payments include:

- **Eye-Vein:** ZTE has integrated EyeVerify's EyePrint ID to some smartphones)
- **Face:** MasterCard are piloting 'Pay-by-Selfie' technology using a combination of facial recognition and voice and Jack Ma, Chairman, Alibaba, showcased a mobile facial recognition solution for Alipay in march 2015
- **Iris:** NTT DOCOMO is using Fujitsu Arrows smartphones that support Iris recognition and are using them for carrier billing payments in Japan. Microsoft Lumia smartphones are planning to use Iris with Microsoft's Hello biometric authentication solution
- **Voice:** Used as part of multi-modal biometric authentication and to enhance liveness detection in facial biometrics

Non-fingerprint biometric modalities offer payment providers and payment card issuers an opportunity to deploy mobile payment services that do not rely on the mobile manufacturers or mobile platform owner's built-in solution and still offer consumers a frictionless method of authorising payments on smart mobile devices. They could also enable retailers to own the payment environment in their own mobile apps.

[3] Taken from the Goode Intelligence analyst report "Mobile & Wearable Biometric Authentication Market Analysis and Forecasts 2014-2019: **http://www.goodeintelligence.com/report-store/view/mobile-wearable-biometric-authentication-market-analysis-forecasts-20142019-2nd-edition**

[4] Taken from the Goode Intelligence analyst report "Biometrics for Payments – Payment Security Gets Personal; Market & Technology Analysis, Adoption Strategies and Forecasts 2015-2020: **http://www.goodeintelligence.com/report-store/view/biometrics-for-payments-payment-security-gets-personal-market-technology-analysis-adoption-strategies-forecasts-20152020** ***(Note that these figures are for all payment types not just Mobile).***

Wearable Payments – Matching the Biometric to the Device

What is imperative to the success of a biometric deployment is choosing the most appropriate biometric modality to match the device and the context of its use. Fingerprint sensors, especially touch sensors, have been so successful for smartphones and mobile payments because touch is such a natural interaction with these devices.

By 2019 over 932 million wearable devices will be sold
Goode Intelligence Forecasts

Payment services providers are turning to wearable devices, especially bands and smart watches, to support payments for in-store transactions.

Biometric identification is currently not supported for wearable payments but there is an opportunity to integrate certain biometric modalities to enable robust user identification.

One biometric modality that is suited to wearable devices is heartbeat biometrics and this is currently available on the Nymi band. Nymi's Heartbeat ID is being used in proof-of-concepts (POC) and pilots by a number of financial institutions a payments pilot with MasterCard and a number of Canadian banks including TD Bank and the Royal Bank of Canada.

It also has the capability to be used to store a user's Bitcoin in a native biometric wallet with the private key tied to a unique ECG biometric signature.

Nymi is the not only vendor using an ECG, **B-Secur** is developing biometric authentication solutions based on this heart-based modality.

The Nymi Band

Biometric Payment Cards – Let's Get Rid of the PIN

The payment card (credit or debit) is one of the most popular ways in which consumers pay for goods and services enabling them to make payments in-store, online and even withdraw cash from an ATM. There are estimates that over 1.5 billion smartcards were used for payments worldwide during 2014.

As a result of its popularity, payment and banking cards have been widely targeted by criminals. The payments industry has responded by introducing security technology to counteract attacks when they happen. One such security technology, 'chip-and-PIN' or 'chip-and-signature'– a result of EMV standards – has resulted in reduced levels of fraud at the retail Point-of-Sale (POS) and ATM.

Card skimming is still possible in POS and ATM machines that have been tampered with as some card issuers will poorly implement EMV or put cardholder data on the magnetic stripe that can be easily read with inexpensive skimming devices.

Card Not Present (CNP) fraud increased by 10% from £301m in 2013 to £331m in 2014 in the UK[5]

A consequence of improved card security has seen increases in fraud cases in payment scenarios where the chip cannot be read – Card-Not-Present (CNP) transactions. This includes telephone and mail-order shopping but more frequently when making payments online (eCommerce). For online, the response from the card industry has been 3D-Secure; an additional layer of user authorisation based on certain characters from a user passcode.

An emerging technology that can be added to the payment industry security toolkit is biometric cards. There are a number of deployment choices for biometric cards, the two main ones being integrating a biometric sensor (usually a fingerprint sensor) into a smartcard and capturing the biometric on an external sensor and then storing the template on a chip card (smartcard).

EMV: Europay, MasterCard and Visa; the three payment schemes that created the EMV standard, a technical standard for smart payment cards. EMV cards store their data on integrated circuits (chips) rather than magnetic stripes. EMV cards can be contact or contactless.

CNP: A card not present transaction is a payment card transaction made where the cardholder does not or cannot physically present the card for a merchant's physical examination.

3D-Secure: Three Domain Server is an additional fraud prevention scheme that involves three parties (retailer, acquiring bank and the card scheme) to reduce eCommerce fraud.

[5] Plastic fraud figures, The UK Cards Association:
http://www.theukcardsassociation.org.uk/plastic_fraud_figures/index.asp

Biometric Cards – Integrated Biometric Sensor

This is emerging technology and currently there a number of vendors bringing their biometric cards to market for banking and payment use. Much of the initial activity is in the payments sector but as most smartcards issued by banks are dual use they can be used to access services from ATMs.

The specialist biometric card companies include **Zwipe, SmartMetric** and **Cardtech.** Zwipe has been involved in payment trials with MasterCard.

Biometric Cards – "Match on Card"

An important catalyst for the adoption of biometric cards in "match on card" mode has been Visa's announcement in September 2015 that they have introduced a new specification to use biometrics with chip card transactions. The specification can enable palm, voice, iris, or facial biometrics. This technology framework is designed to work with the EMV chip industry standard to help ensure open, globally interoperable solutions. The architecture Visa has designed enables fingerprints to be securely accepted by a biometric reader, encrypted, and then validated.

The specification supports "match-on-card" authentication where the biometric is validated by the EMV chip card and never exposed or stored in a central database. Issuers can optionally validate the biometric data within their secure systems for transactions occurring in their own environments, such as their own ATMs. Visa will offer to contribute the technology to **EMVCo**, the global technical body that manages the EMV Specifications, to further develop and administer the standard for the benefit of the entire payment industry.

Outlook

There may be a shift towards the use of mobile and wearable devices for payment purposes but banking and payment cards are a dominant form of payment and, like cash, will be used by hundreds of millions of people worldwide for many years to come. Biometric cards are an evolutionary security feature and will play an important role in improving usability and reducing fraud. Biometric Payment card forecasts are included in Goode Intelligence's Biometric for Payments analyst report.

Biometric Innovation at the ATM – Card-less Cash Dispensing

Cash is going nowhere anytime soon and is still a very important form of payment. Ensuring that customers can conveniently and securely access their bank accounts to get cash from ATMs is incredibly important.

Unfortunately where there is money there will be criminals intent on defrauding customers of their hard-earned cash. Financial institutions and ATM network providers must ensure that they implement enhanced security mechanisms to prevent fraudulent access to their customer's bank accounts when using ATMs. Card skimming, distraction and coercion attacks all undermine the ability for them to do so.

One such security mechanism is being provided by biometric authentication platform provider **Hoyos Labs**. The company is the inventor of the **IEEE Biometric Open Protocol Standard (BOPS)** and has adopted this standard for their biometric authentication platform, including the HOYOSID biometrics-based identity assertion identity platform.

In an attempt to solve the problem of ATM Skimming, Hoys Labs has developed a mobile-based biometric solution that allows bank customers to withdraw cash using smartphones.

Hoyos Labs 1U™ ATM is a software platform that allows bank customers to access their accounts via ATMs using biometrics on smartphones. There is no need for cards or for the customer to enter in a PIN at the ATM as the entire authentication occurs on the customer's smartphone.

It works by using facial recognition in a mobile biometrics app supplied by Hoyos Labs:

1. ATM customers scan a verified QR code that is displayed on the ATM screen using their smartphones
2. They are then prompted to authenticate themselves biometrically using facial recognition (using the smartphone's camera)
3. Once they have been authenticated they can then use the ATM to access services and withdraw cash

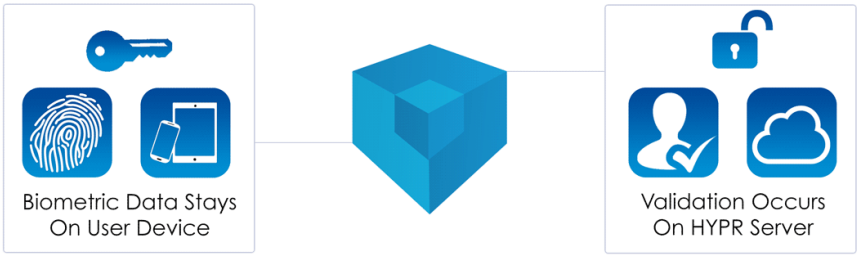
The Hoyos Labs solution is compatible with existing ATM platforms and does not need any hardware to be installed on the ATMs.

Can We Learn from Payment Security? Biometrics Tokenization

Payment tokenization has played a major part in securing stored card data and has played an important role in enabling secure mobile payments, including Apple Pay.

Tokenization is a security mechanism that has prevented sensitive payment data, including a card primary account number (PAN), from falling into the wrong hands. Biometric data, including templates, is also very sensitive data and must be protected at rest and in transit. Biometric data will be attacked and there will be occasions, as with the case of the hack on the Office of Personnel Management that led to millions of US government fingerprint records being stolen, when biometric data is stolen.

Can the Biometrics industry learn from the payment sector and tokenize valuable biometrics data. One vendor that has developed a biometric tokenization platform is **HYPR Corp**.



The platform does not store biometric data on a centralised server and uses a combination of biometric signatures and public key cryptography to support end-to-end biometric tokenization. The HYPR platform is built on four guiding principles that the company calls *The Four Laws of Biometric Tokenization*:

1. No third party should be allowed to centralise storage of biometric credentials
2. Biometric data should remain isolated from the Operating System on a user's device
3. End users should have full control in choosing what biometric authenticators they will utilise
4. Relying parties should be able to choose between BYOD or specialised tokens for authentication

The company has created a solution to secure Bitcoin and other digital currency platforms. The HYPR biometric security platform could be used to biometrically validate Bitcoin transactions. The vast majority of Bitcoin breaches involve the theft of private keys. The proper storage and access to these private keys is of the utmost importance, but unfortunately, most private keys are protected with passwords. Time and again, passwords have proven grossly insufficient for security. HYPR allows for a password-less experience with added security controls, however, which means this type of breach could be avoided.

Tokenization:
The process of substituting sensitive card data with a non-sensitive equivalent, referred to as the token. For Payment Tokenization the PCI Council defines it as "a process by which the primary account number (PAN) is replaced with a surrogate value called a token"

SUMMARY

Innovation in biometric technology is providing payments with a particularly personal security experience and enabling new methods in which we pay for goods and services in a variety of payment scenarios.

It's not about if biometrics are adopted to protect payment services but when and if traditional payment service providers do not adopt biometrics then it is a question of how long they can remain relevant

Biometric systems are being adopted across a wide range of payment types in all parts of the world; from traditional, including cash, to emerging methods that leverage consumer technology, mobile and wearable devices.

Emerging payment solutions are leveraging biometric security to gain a market edge and traditional payment providers are investigating how biometrics can keep them competitive and even to remain relevant.

This white paper has used content from the Goode Intelligence analyst report entitled "**Biometrics for Payments – Payment Security Gets Personal; Market & Technology Analysis, Adoption Strategies and Forecasts 2015-2020**".

BIOMETRICS FOR PAYMENTS – PAYMENT SECURITY GETS PERSONAL; MARKET & TECHNOLOGY ANALYSIS, ADOPTION STRATEGIES AND FORECASTS 2015-2020

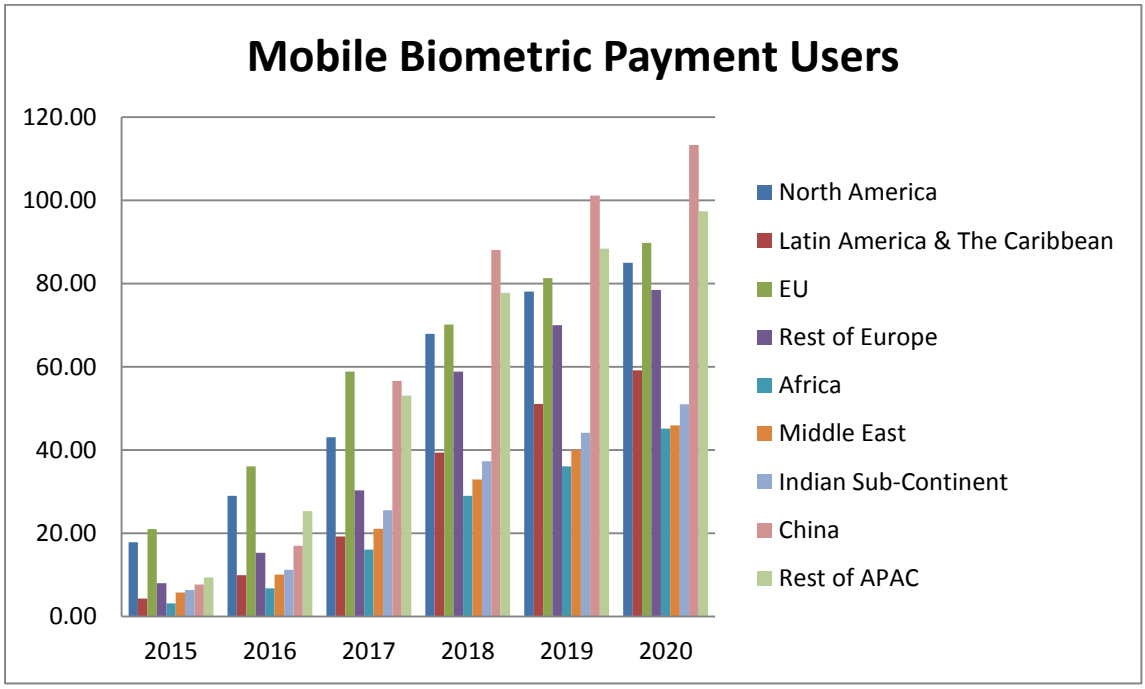
Biometrics for Payments – Payment Security Gets Personal; Market & Technology Analysis, Adoption Strategies & Forecasts 2015-2020 is a 243 page analyst report that provides detailed analysis of the adoption of biometrics for payments.

This comprehensive report includes a review of current global adoption, market analysis including key drivers and barriers for adoption, interviews with leading stakeholders, technology analysis with review of key biometric technologies and profiles of companies supplying biometric systems for companies operating in the payments industry plus forecasts (regional and global) for users, revenue, transaction volume and value within the six-year period 2015 to 2020.

The report investigates the global adoption biometrics by banks across traditional and emerging payment types including *In-store (Biometric integrated POS terminals), eCommerce Payments, Mobile Payments, Wearable Payments, Bitcoin and ATMs.*

Goode Intelligence reveals the most popular biometric technologies that are being adopted across each payment type and introduces emerging biometric systems that are beginning to be piloted by some of the most innovative financial institutions across the world; these include F*ingerprint, Voice, Behavioral, Face, Finger-Vein, Palm Vein, Eye (Iris and Eye-Vein) and Heart.* Mobile Payments has been one of the driving forces for biometric adoption for payments and has been in instrumental for explosive growth for the vendors that are serving this sector – see user forecast for the adoption of mobile biometric payments in Chart 1 below.

Chart 1: Mobile Biometric Payment Users (m)



ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consultancy services in information security including:

- Biometrics
- Mobile Security
- Financial Services Security
- Authentication and Identity
- Internet of Things Security

For more information on this or any other research please visit www.goodeintelligence.com.