GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Biometrics - An important tool for the customer-first bank

A white paper published by Goode Intelligence

www.goodeintelligence.com

First Edition June 2015

Published by:
Goode Intelligence
United Kingdom

www.goodeintelligence.com
info@goodeintelligence.com

CONTENTS

Banks are increasingly deploying biometric systems across a wide range of channels. This white paper from research and consultancy company Goode Intelligence (GI) explores what is driving banks to adopt biometrics, drawing on recent published research on biometrics for banking.

FRICTIONLESS AUTHENTICATION AND FRAUD REDUCTION – TWIN-DRIVERS FOR THE ADOPTION OF BIOMETRICS IN BANKS

Banks that have put the customer at the heart of their business strategy are increasingly turning to biometric technology in an attempt to improve the authentication user experience and reduce financial fraud.

Banks and their partners are either planning to or deploying biometric technologies across a wide-range of bank channels including ATMs, in bank branches, to support telephone banking, for electronic (web based) banking, within mobile banking apps and beginning to work with innovative biometric vendors for pilots and proof-of-concepts (POC) in wearable devices.

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

ATM: Automated Teller Machine.

IVR: Interactive Voice Response.

A major shift in attitude at banks – Biometrics; part of the strategic effort to reduce fraud and friction across all banking channels

CUSTOMER IDENTIFICATION FOR THE OMNICHANNEL BANK

Goode Intelligence believes that one of the main reasons for banks to adopt biometric technology is the need for convenient privacy-aware authentication across a number of banking channels with the emergence of mobile as the prime banking channel and emergence of wearable banking strategies.

The question that banks are asking is "how do we ensure that our customers are adequately identified when accessing bank services at all bank access points" – customer identification for the Omnichannel bank.

A hardware OTP token or smartcard works well enough when a bank customer is accessing banking services from a desktop computer at home but is inconvenient when that same customer is using their mobile phone or calling up their bank using a telephone-based service.

These 1980s two-factor authentication technologies are also susceptible to Man-in-the-Middle (MitM) and Phishing/Malware attacks.

Bring Your Own Fingerprint – BYOF

Biometric-enabled mobile devices allow banks to roll-out biometric authentication to millions of customers without the added cost of additional hardware

This has led banking professionals to look for alternatives that meet the needs to strongly authenticate across a wide range of existing banking channels; ranging from wearables, the very new, to technology like the ATM that has been around since the late 1960s.

According to Angel Grant, Senior Manager, Fraud and Risk Intelligence, **RSA Security,** "banks are looking for an Omnichannel approach where the same biometric modality or system is used across

OTP: One-Time-Password. A cryptographically created single use passcode that can be created by hardware or software tokens.

MitM: Man in the Middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. It can lead to theft of authentication credentials.

Phishing: An attempt to acquire sensitive information including username and password details by masquerading as a legitimate entity.

channels". This could be a difficult challenge for banks as different biometric modalities may be better equipped to deal with fraud and authentication in separate channels. RSA is attempting to bridge this gap by tighter integration across security services including authentication and fraud management solutions. RSA has recently launched its new family of smart identity solutions, **Via**, that aims to link authentication, governance, security intelligence/analytics with adaptive (risk-based) authentication. The platform along with RSA Adaptive Authentication mobile SDK also supports biometrics, initially with Touch ID fingerprints and voice on supported devices but eventually to other modalities that could support the differences required to manage authentication across all bank channels. This platform approach could be the solution to ensure that the most appropriate biometric modality is linked to the right banking channel.

SDK: Software Development Kit is a set of development tools that allows the creation of applications for software/hardware solutions.

This platform approach could be the solution to ensure that the most appropriate biometric modality is linked to the right banking channel

FinTech: Financial Technology is a business based on technology to provide financial services.

Opportunities for Challenger Banks

The explosion of FinTech-led financial services has also meant that challenger banks, like **Atom Bank** in the UK and **Bankmobile** in the USA, are looking at innovative ways that customers can interact with their banks; biometrics gives them the potential to offer their customers a usable and secure method to protect their financial assets when accessing financial services from a range of endpoints.

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

WHICH BIOMETRIC AUTHENTICATION SYSTEM IS RIGHT FOR BANKS?

The use of integrated fingerprint sensors is just one method of providing convenient banking user authentication and will continue to grow as more devices become available. The device-centric model of Apple's Touch ID and FIDO is proving to be popular for banks wanting to quickly role out biometric authentication for mobile banking apps.

FIDO: The FIDO Alliance is an organization that has developed authentication standards and specifications to improve online authentication for both mobile and desktop computing experiences.

Multi-modal biometric authentication supporting a *member first* strategy

However, Goode Intelligence believes that these solutions will evolve and increasingly incorporate other authentication factors and biometric modalities to provide strong security and convenience. For instance, by combining face and voice in a multi-modal biometric authentication

solution that can work across a range of banking channels. **USAA's** recent deployment of **Daon's IdentityX** multi-modal mobile authentication platform is a great example of this and backs-up USAA's '*member first'* strategy.

Combination of context and security risk drives the choice of biometric system

Depending on the context of the transaction/interaction, you can either use a single modality - voice in a telephone banking interaction - or a combination of modalities - face and voice for mobile or desktop banking services.

Combination of context and security risk will dictate most-appropriate modality or factor to use

The security measures needed to protect a high-value, multi-million dollar, corporate bank transaction will be different than that offered to a retail customer checking their balance on a mobile device; the combination of context and security risk will dictate the most-appropriate modality or factor to use.

Biometrics does have the capability of protecting higher-value banking transactions but must meet more stringent security requirements to reduce the risk. For instance, a retail bank may leverage Apple's Touch ID fingerprint biometric system to enable customers to sign-in to the mobile banking app on their iPhones but will probably not use the same solution to authorise a multi-million dollar intra-bank transaction. Use of a dedicated high-end fingerprint sensor attached to a corporate banking employee's terminal using strong authentication protocols would be considered to be appropriate.

Banking Biometric System Assessment

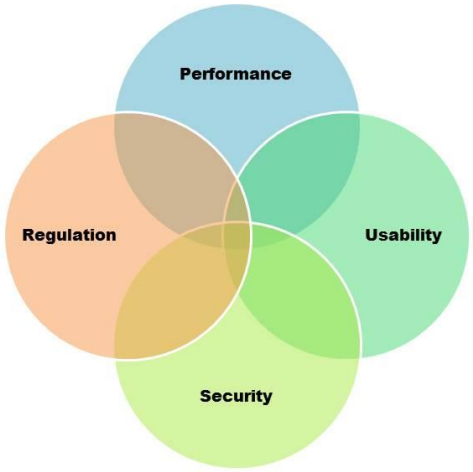
Goode Intelligence provides biometric and authentication consultancy services to banks and works with them in assessing and choosing the most appropriate biometric system or modality to meet their requirements.

Based on this experience and our work with biometric and authentication technology companies, Goode Intelligence has devised an assessment tool that banks and systems integrators can use to ensure that the most appropriate biometric system is chosen. The Goode Intelligence ***Banking Biometric System Assessment (BBSA)*** tool is based on four interlocking parts, ***biometric performance***, ***usability***, ***regulation*** and ***security***.

Biometric Modality: A biometric modality is a type or class of biometric system. Modalities include fingerprint, face and voice for instance.

BBSA: Banking Biometric System Assessment is Goode Intelligence's biometric assessment tool designed for the banking sector.

Figure 1: Goode Intelligence Banking Biometric System Assessment (BBSA)



Source: Goode Intelligence © 2015

On-device versus cloud-based biometric systems

There are various biometric system architectures that a bank can adopt including device-centric, where the biometric data never leaves the device, or server-centric (sometimes offered as a Biometric as a Service), where the user enrols their biometric and then is stored by the financial institution (or technology service partner). For verification; the matching is performed on the device for the device-centric model and against a stored template within a network database for the server-centric model.

Goode Intelligence believes that both models have their merits and feel that the decision to adopt one over the other (and there will be scenarios where a mixture of both will be adopted) will be driven by a combination of privacy/trust requirements and specific business drivers (some of which will be moulded by culture decisions, i.e. availability of national biometric database).

For on-device biometric authentication services, where the device is predominantly a smartphone, we believe that the best approach that meets privacy and trust requirements is to utilise embedded security within mobile devices; Secure Enclave for iOS and **TrustZone** in ARM-based devices.

A great example of this is voice biometric specialist **AGNITiO's** VOX ID Mobile solution that leverages TrustZone embedded hardware security using a FIDO-Ready implementation developed by **Nok Nok Labs**. In this model, the bank customer enrols their voice print on a smart mobile device and then be able to access mobile banking services securely using their voice for authentication. AGNITiO also support the server-

Secure Enclave: The Secure Enclave is Apple's secure area of a chip that is used to securely store credential data including fingerprint data. The Secure Enclave is 'walled' off from the rest of the chip and the rest of iOS. Only Touch ID currently uses it.

TrustZone: TrustZone has been developed by chip designer ARM and is a secure part of an ARM chip that can be used to securely store secure data and applications. It can be used to store biometric data including templates.

OEM: Original Equipment Manufacturers are manufacturers who resell another company's product under their own name and branding. For instance, Samsung sell smartphones based on Google's Android operating system. This is sometimes referred to **ODM** or **Original Design Manufacturer**.

centric and IVR-based models ticking the boxes to support Omnichannel banking.

SUMMARY

Goode Intelligence expects to see a lot of innovation in this space where bank-controlled multi-modal biometrics based on the server-centric model will compliment device-centric models with integrated mobile biometric solutions offered by mobile OEM enabling customers to securely access full-banking services from a wide variety of end points.

There will be many different models for adoption of biometrics in banking – It is not just about integrating Touch ID into your mobile banking app

Biometric systems are being adopted across a wide range of bank channels and services in all parts of the world. Goode Intelligence believes that adoption is accelerating and will result in biometrics being the predominant method to identity bank customers by 2020.[1]

[1] ***Biometrics for Banking; Market and Technology Analysis, Adoption Strategies and Forecasts 2015-2020***. Published by Goode Intelligence on 1st June 2015: **http://www.goodeintelligence.com/report-store/view/biometrics-for-banking-market-technology-analysis-adoption-strategies-forecasts-20152020**

BIOMETRICS FOR BANKING; MARKET & TECHNOLOGY ANALYSIS, ADOPTION STRATEGIES AND FORECASTS 2015-2020

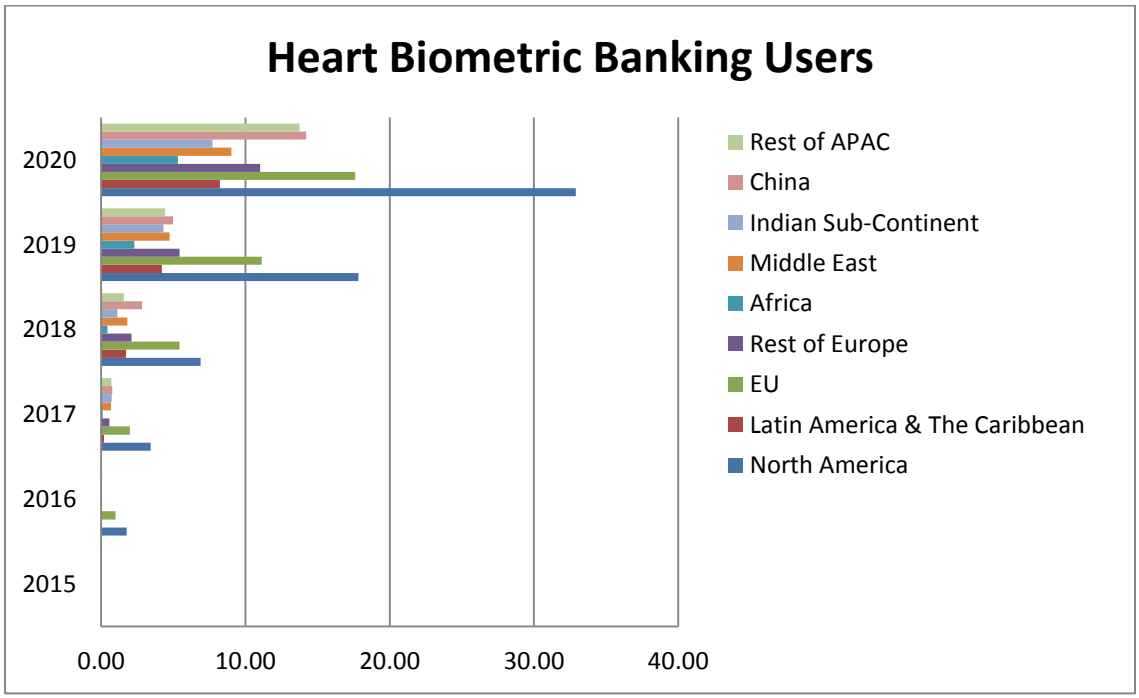
Biometrics for Banking; Market & Technology Analysis, Adoption Strategies & Forecasts 2015-202 is a 238 page analyst report that provides detailed analysis of the adoption of biometrics for banking.

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 to banks plus forecasts (regional and global) for users and revenue within the six-year period 2015 to 2020.

The report investigates the global adoption biometrics by banks across traditional and emerging bank channels including *Bank Branch, Electronic Banking (web-based), Telephone Banking, Mobile Banking, Wearable Banking and ATMs.*

Goode Intelligence reveals the most popular biometric technologies that are being adopted across each banking channel and introduces emerging biometric systems that are beginning to be piloted by some of the most innovative banks across the world; these include F*ingerprint, Voice, Behavioral, Face, Finger-Vein, Palm Vein, Eye (Iris and Eye-Vein) and Heart.* Heart biometrics is at its very early stages of being adopted and Goode Intelligence believes that it will have a very important part to play for banking in the next generation of wearables – see forecast for the adoption of heart biometrics in bank in Chart 1 below.

Chart 1: Heart Biometric Banking User Forecasts (m)



Source: Goode Intelligence © 2015

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
- Banking Security
- Authentication and Identity
- Internet of Things Security

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