GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

White Paper

Mobile Biometrics
Reducing Fraud & Customer Friction for Financial Services

Mobile biometrics has transformed how financial service providers identify and authenticate their customers, enabling them to dispense with inconvenient technologies that have been shoe-horned to work on smart mobile devices.

The need for speed and the removal of friction from a range of financial services has created the demand for alternative identity solutions that can operate in a range of channels from traditional (ATM) to the latest digital financial services (mobile, web and IoT).

CONTENTS

MOBILE BIOMETRICS – REDUCING FRAUD & CUSTOMER FRICTION FOR PAYMENTS AND BANKING

Mobile biometrics has transformed how financial service providers identify and authenticate their customers, enabling them to dispense with inconvenient technologies that have been shoe-horned to work on smart mobile devices.

The need for speed and the removal of friction from a range of financial services has created the demand for alternative identity solutions that can operate in a range of channels from traditional (ATM) to the latest digital financial services (mobile, web and IoT).

The delivery of financial services is being transformed by a series of digital mega-events that include the *Open Banking* revolution where banks and payment services providers are being forced, either by regulation such as the EU's PSD2 or by pressures from FinTech providers, to open up their digital infrastructure to third parties using APIs.

Tied to open banking is the need for seamless methods for financial services providers to engage with their customers and to prove who they are – *identity* – so that they have a convenient method to gain access to their authorised banking services – *authenticate* – to make payments *any time any place anywhere* (the Martini principle) and to ensure that fraud levels are kept at acceptable levels – *fraud management*.

Identity verification, authentication and fraud management are the three inter-connected areas that mobile biometrics is really establishing itself as an important tool for banks and payment services providers to deploy.

Our analysis of the current market, estimates that by the end of 2023 some 1.7 billion bank customers will be using mobile biometrics to withdraw cash from ATMs, to prove their identity when contacting their bank via the telephone (both actively and passively), proving their identity for digital onboarding using their face, authenticating into their mobile bank app using their fingerprint and using a combination of their face and voice to initiate money transfers when accessing web-based eBanking services.

1.7 billion financial services customers using mobile biometrics by the end of 2023

Mobile Biometrics – Reducing Fraud & Customer Friction for Financial Services

The major trends that Goode Intelligence is seeing for this industry include:

- Rise of mobile & multi-modal mobile-based biometric authentication

- Biometric adoption in all channels supported by open banking APIs that support biometrics

- Beginning of the deployment of single biometric platforms leveraging mobile biometrics to support multiple channels and identity, authentication and fraud management functions

- The growth of biometric identity verification (proofing) harnessing mobile face biometrics

- Industry regulation starting to specifically reference biometrics as part of its guidance on two and multifactor authentication (EU PSD2, USA FFIEC guidelines and Bank of China and Korea legislation)

- The growth of mobile face biometrics as a biometric technology that is versatile and can support identity verification and authentication

- Leveraging the power of machine learning (ML) and Artificial Intelligence (AI) technology to improve biometric performance and spoof / liveness detection – both in-chip (on-device) and in-cloud

- FIDO 2.0/WebAuthn standards and support by major browsers will accelerate mobile-based FIDO authentication for banking and payments

An area where we are seeing increasing adoption for mobile biometrics is that of electronic identity and document verification (eIDV).

BIOMETRICS AND IDENTITY AND DOCUMENT VERIFICATION

Biometrics is increasingly being used to aid online identity verification, often called proofing, especially to facilitate digital on-boarding for new bank account opening. In accordance with AML and KYC regulation, a bank needs to verify the identity of people wanting to open up a new account or banking service. Traditionally, you needed to physically present trusted identity documentation such as passports, driver's licences or national identity documents, alongside proof of address – usually in the shape of a utility bill. For banks seeking to streamline this process and move identity verification online (digitally) the AML and KYC regulations proved problematic.

To enable digital customer on-boarding and to comply with AML and KYC regulations, banks are turning to a combination of electronic document and identity verification (eIDV) and biometric identification.

Part of the on-boarding process, electronic identity (eIDV) and electronic document verification (eDV) plays an important part in validating the identity of a new customer and meeting AML and KYC regulation.

eIDV and document verification can also be used outside of the customer on-boarding process.

Currently, eIDV works in the following ways:

1. Capturing user data during registration process the eIDV service will verify the identity data, including first name, last name, national ID, social security number, address, data of birth and telephone details from multiple data sources

2. In addition to 1, document verification where an image of a trusted identity document is captured by the registering customer and this is validated against multiple data sources

Electronic Identity Verification (eIDV) enables organisations to verify the identity of applicants and customers by collecting personal information from them that can be verified against a number of data sources.

Personal information can include:

•   First name

•   Last name

•   National ID

•   Social security number

•   Address

•   Data of birth

•   Mobile number

Document verification is designed to enable digital account opening by scanning and verifying an applicant's physical ID – a driver's licence, national ID card or passport. It is better suited to mobile use as most mobile phones have adequate cameras for photo ID capture.

An applicant takes a picture of the photo ID and the document verification solution verifies that the captured information is valid. The data from the card can also be used to pre-populate an application form.

Electronic document verification (eDV) has a link to biometrics in the form of validating a person's 'live' face against that stored in a trusted document. The majority of the current eDV solutions do not capture the person's face during the eDV process but there is an opportunity to do so and then subsequently use this in the user authentication process to verify the document and authenticate the person. It has the ability to tighten the verification process and reduce the risk of a fraudster either using a fake or stolen photo ID.

The eIDV and biometrics digital on-boarding market is particularly buoyant at the moment with many vendors and service providers offering services to a range of businesses including banks.

MOBILE BIOMETRICS FOR FINANCIAL SERVICES; MARKET & TECHNOLOGY ANALYSIS, ADOPTION STRATEGIES AND FORECASTS 2018-2023

The second edition of **Mobile Biometrics for Financial Services – Market & Technology Analysis, Adoption Strategies & Forecasts 2018-2023** is a 206 page analyst report that provides detailed analysis of the market and adoption of mobile biometrics for financial services.

The report includes:

1. Review of current global adoption
2. Market analysis, including key drivers and barriers for adoption across a wide range of financial services including payments and banking
3. Technology analysis
4. Analysis of important technology vendors and services providers operating in this sector
5. Forecasts for users and revenue within the six-year period 2018 to 2023

Biometric vendors are experiencing tremendous growth on the back of the escalation of consumer-led adoption of mobile biometric authentication. The adoption for financial services purposes is a major contributor to this growth and Goode Intelligence forecasts that by 2023 it will contribute US$8.7 billion in revenue for companies involved in delivering mobile biometric systems for financial services.

Mobile biometrics is increasingly a vital part of a financial service provider's toolkit in the never-ending task of reducing financial fraud and ensuring that their customers can conveniently prove their identity when accessing financial services – smarter identity verification and authentication for the customer-first organisation.

Mobile Biometrics - Smarter Identity Verification, Fraud Detection and Authentication for the Customer-First Financial Services Provider

ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has established a strong reputation for providing quality research and consultancy services in digital identity, authentication and biometrics.

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

This document is the copyright of Goode Intelligence and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Goode Intelligence.

ABOUT GOODE INTELLIGENCE