Guidelines for Deploying Mobile Biometrics in Financial Services

opusresearch
Biometrics are proving to be a superior way to authenticate and make digital financial services more secure, but organizational implementations are lagging. As biometrics are more widely adopted by consumers for financial and non-financial use cases, banks are challenged to match higher user experience standards. In this document, Opus Research discusses findings from a joint report by Mastercard and the University of Oxford offering key insights for business, customer experience and systems owners to consider when deploying mobile biometrics including a prescriptive checklist for implementation, strategy, and tactics.

Biometric Implementations Fall Short of Potential

Research reports have long projected biometrics to deliver strong, multi-factor consumer authentication. For example, Mobile Biometrics Market has forecast a CAGR of 29.3% for the period 2016-2022. Still, despite these positive projections, actual adoption is sluggish in relation to the tremendous growth in biometric-enabled smartphone penetration. So, what is the key to unlocking the commercial, security and customer value of biometrics for widespread adoption?

Oxford/Mastercard Report Reveals Key Factors Influencing Adoption

Mastercard collaborated with Oxford University to explore and address the factors that currently appear to inhibit the adoption of biometric authentication. Findings were published in a report entitled “Mobile Biometrics in Financial Services: A Five Factor Framework.” Based on new primary research, as well as recently published secondary sources, its authors delve into issues affecting deployment plans, strategies and tactics. The study confirms consumer preference for secure and user-friendly authentication, but also reveals a lack of knowledge among key industry professionals and bank decision makers. These gaps appear to further exacerbate perceptions of and challenges associated with the effective utilization of mobile biometrics.
A More Holistic Approach to Deploying Mobile Biometrics

The first step in the successful implementation of mobile biometrics projects is recognising the multiple dimensions associated with designing, implementing, operating and continuously improving implementations. Specifically, for financial services, we reference the Five Factor Framework, outlined by Mastercard and Oxford University, as an aid for key decision makers and industry stakeholders to improve collaboration based on a common, comprehensive structure.

Passwords are Passé, Yet Prevalent

Since most mobile authentication is still being conducted through PIN/password mechanisms (Cybersecurity Ventures & Thycotic estimate passwords to grow from 90 billion today to 300 billion by 2020), the trade-off between usability and security, especially at rapidly growing scale, is of growing concern. The U.S. Commission on Enhancing National Cybersecurity hopes to see “no major breaches by 2021 in which identity, especially the use of passwords, is the primary vector of attack.” This is an ambitious goal as 81% of all successful data breaches can be tracked back to inadequate passwords according to Verizon’s 2017 Data Breach Investigations Report.

The next most popular authentication method in mobile commerce is token-based, primarily that of one-time-pin (OTP) which is typically sent to a consumer via an SMS message This, too, is under scrutiny due to various security risks.
Biometrics Solves Mobile Authentication Shortcomings

A recent LexisNexis ‘Cost of Fraud’ study revealed that digital fraud is growing at the same rate as digital commerce, and when one considers that the various fraud loss projections are expected to exceed tens of billions of U.S. dollars by 2020, two key components for digital customer authentication need to be simultaneously addressed: usability and security. Biometrics addresses both of these by virtue of its ease of use, delivered through multiple layers of security.

The growth of mobile banking, shopping and payments is fueling accelerated growth in the use of biometrics as a convenience feature for end users and as a security feature for businesses.

Many Banks Already Benefit from Biometrics

Various biometric modalities, such as finger, face, iris and voice, are currently in use across a variety of banks. To name a few, these include Bank of Scotland, BBVA Compass, Deutsche Bank, HSBC, Lloyds Bank, Mashreq, Santander USA, Standard Chartered, ABN AMRO, JP Morgan Chase, OCBC, Banco Inbursa, Gulf Bank, Nequi, Tangerine, Simple (BBVA), Wells Fargo, Natwest, Investec and many more. When Opus Research conducted its most recent Census of Voice Biometrics Implementations in late 2016, we discovered that more than 135 million people around the world had enrolled for services that would use their voice to speed up the authentication process. Clients and customers of banks and financial services companies accounted for over half of this enrolled population. The 135 million figure represented an 84% annual growth rate during the two prior years. Banks saw a commensurate increase in efficiencies through reduced call handling times, and even improved first call resolution from greater authentication successes. This, together with the Oxford/Mastercard findings, suggest that mobile-based biometrics, too, will be accepted and anticipated to yield immense business benefits.

There is also a growing application of multi-modal biometrics, where solutions that provide customers the choice to use fingerprints, voice or facial recognition have been showcased by financial services giant USAA in the United States as well as “challenger” Atom Bank in the UK which regards the use of leading-edge technology as a differentiator in an increasingly competitive banking environment.
Oxford/Mastercard Discovers a Knowledge Gap in Banking Organizations

The Oxford/Mastercard study reveals fundamental knowledge gaps in the financial services industry; with 88% of business professionals expecting to be involved in making key decisions relating to implementing mobile biometrics, yet only 36% claiming to have adequate experience. An overwhelming 64% of technical professionals claim to have little or no experience. This appears to be one of the key inhibitors to action, since 92% of the industry is interested in deploying but only 13% have already done so.

To address these knowledge gaps, the Oxford/Mastercard research structures mobile biometric considerations into 5 key themes (“Five Factor Framework”), against which Opus Research highlights some of the key ideas and implementation best practices gathered from industry bodies and academia.

Designing for Success

As initial implementations of biometrics in financial institutions have shown, authentication touches almost every element of any customer-centric organisation. As such, this requires collaboration across multiple departments, and the involvement of team members who possess a solid understanding of the relevance of a complex set of considerations in making responsible and effective implementation decisions. These priorities and considerations are made clear through the Five Factor Framework:

I. Modality Performance

The Oxford/Mastercard study cautions against overstating the importance of modality performance, which measures the quality of the biometric ‘engine’. Most commonly, this performance is expressed in terms of False Accept (“FAR”) or False Reject (“FRR”) rates, often combined as to create Equal Error Rate (“EER”) or Receiver Operating Characteristic (“ROC”) curve. There is a general tendency for decision makers to gravitate towards these measures due to their relative ease of quantification and comparison across vendor products. Yet, the biometric engine, despite being the heart of the system, is only one of many components that make up the overall solution. Various other elements, especially in the mobile context, impact overall solution success and are of similar priority to modality performance, as follows.

II. Usability

Usage of biometrics has historically been led by government institutions, with marginal consideration for usability as adoption has generally been enforceable. Even the more recent FIDO UAF (Fast Identity Online, User Authentication Framework) and BOPS (Biometric Open Protocol Standard, IEEE 2410 IEEE Standard) give very little attention to usability. Simple, intuitive usability is key to driving biometric adoption, as users need to be empowered to become fully self-sufficient as easily and quickly as possible. Traditional analysis methods employed in controlled environments with relatively small samples of participants are inadequate to provide practical insights regarding mobile biometric usage, which happens in diverse and unsupervised environments. Studies therefore need to be designed for high-scale, automated observation and feedback.

Different biometric modalities require different user understanding and behaviors. Further, the modalities placed within the context of different channels, user devices and applications make usability design quite complex. To overcome this complexity, usability needs to be broken down into simpler concepts (or goals; summarized by NIST as effectiveness, efficiency, satisfaction, learnability and memorability).

The Oxford/Mastercard report also provides insights on the role of pre-existing user perceptions and biases regarding the use of these technologies (fingerprint, selfies) that businesses should account for as part of their communications/user training to ensure optimal adoption.
Where possible, usability should strive for zero-effort with passive and continuous measurements. Ideally, only request explicit biometric interaction in cases where the confidence level needs to be high or user consent is needed (e.g., when transferring funds or granting access to very sensitive data). In addition, the move toward the use of risk-based decisioning by banks exacerbates the problem of password memorability, further supporting the case for biometrics.

III. Interoperability

According to Globalwebindex, a typical digital consumer owned 3.64 connected devices in 2016; and this figure is growing especially with the surge of Internet of Things. Hence the need for device interoperability increases in importance. Modern biometric deployments need to be capable of handling various devices, biometric modalities and use cases. While centralized template storage and matching supports most interoperability requirements, this approach requires management of data security and associated potential reputational damage risks in addition to diverse biometric sensor data quality.

Device side storage minimizes the data security risks. Implementation of higher level identity architectures that group multiple devices under one user umbrella allows such designs to achieve all these forms of interoperability.

IV. Security

One of the most important tasks when designing the security of a biometric authentication system is the evaluation of the threat model to anticipate the likely form of attacks. Conventionally, the false accept rate (FAR) is relied on as the primary measure of system performance. However, FAR is not fully suitable for large deployments of mobile-based biometric solutions. FAR also only accounts for the success rate of zero-effort attacks (i.e., attacks by fraudsters who have no knowledge of the victim) and without any significant presentation attack (PA) of the victim’s features.

At the very least, real-life threat models for mobile biometrics should incorporate PA, in which case counter measures or anti-spoofing measures would be implemented, such as:

- Measuring physiological properties of the individual (e.g., blood pulse or pressure, spectral or optical properties of the skin),
- Identifying human behavioural responses (e.g., blinking, pupil or head movement),
- Challenge-response protocols (e.g., the system presents a challenge to the user that is different at each authentication attempt).

Manage Malware and Mobile App Attacks On-device

In the case of mobile apps and distributed biometric processing, the end device and client applications become the more likely target of attacks. Malware can, at a large scale, intercept or alter the information or outcome of biometric authentication processes on mobile devices, thereby presenting a serious scalable threat. It is therefore essential that malware and rooting detection capabilities be built into any distributed model, together with using the best available on-device security capabilities. Additionally, mobile app development should include code obfuscation, runtime measures, white box crypto and attack-aware security.
Enrollment Best Practices
The enrollment of biometric templates against weak or false identity attributes is one of the most fundamental threats to biometrics in general. All too often, identity assertion is overlooked during the initial project stages, due to the emphasis placed on pure technology aspects, and reactively introduced as an afterthought. The temptation is to apply existing authentication methods as the easiest solution to authorize enrollments.

Banks typically collect and validate consumer information through physical and “know your customer” (KYC) methods prior to opening of accounts. This is inconsistent with biometric enrollment, which is typically done remotely. Greater integration of these two processes will benefit all stakeholders. Banks should adapt conventional identification and verification (ID&V) for stronger authentication prior to enrollment, including the use of third-party and ‘rooted’ information sources such as government entities as well as the growing variety of other government and private sector initiatives to provide federated identity services.

V. Privacy
Privacy concerns are heightened as biometrics gain popularity. From a regulatory perspective in the EU, there is increased support for biometrics in online payments. For example, the Revised Payment Services Directive (PSD2) will allow retailers to retrieve customer information from banks, but only with consumer permission enabled by far stronger security checks. Furthermore, the General Data Protection Regulation (GDPR) requires the explicit consent of the user for the use of their biometric data, which will also most likely involve improved levels of authentication, ensuring that it is clearly transparent to the user what rights they are granting.

Responsible adoption of privacy-preserving technologies, self-regulation to ensure data security, and mutual education of industry and regulators will be important to the continued innovation and adoption of biometric technologies.

Mitigate the Impact of Data Breaches
According to the Oxford/Mastercard study, reputational damage is overwhelmingly the top concern of bank respondents (75%), followed by fears that data leaks could stop their customers from using the biometric system (72%). It is therefore vital that biometric systems are designed with careful consideration of the measures to mitigate data breaches. Many of the respondents reported distributed models as an architectural choice that would mitigate this concern. Having hardware/software separation between financial and identity data will further mitigate risk.

Methods for Protecting Biometric Templates
Due to the need to accommodate for slight variances in biometrics due to aging, environment and noise, traditional cryptographic methods such as hashing and salting, commonly used for more static data such as passwords, cannot be used to protect biometric data. Methods that apply template transformation to the biometric image before it is stored, and biometric cryptosystems are utilized to increase protection from attackers. These methods enforce:

- **Noninvertibility** – Safeguarding against retrieving the original biometric template from its protected reference
- **Revocability** – Tactics against obtaining the original biometric template from multiple instances of the protected biometric reference derived from the same individual
- **Nonlinkability** – Methods to inhibit discovering whether two or more instances of the protected biometric template were derived from the same biometric trait of a user
On-device Solutions Appear to Have Greater Advantages
While FIDO UAF and BOPS do not mention template protection, the use of secret keys that are bound to three elements – user account, user device, and third-party application – have the following advantages:

- **Large-scale transmission and storage of sensitive data over networks is minimized**
- **Keys are not shared between third parties, hence data cannot be linked between third parties**

This, together with consumer preference for device interoperability, which may be addressed through device householding, makes on-device solutions more suited for mobile biometrics.

Achieving Mobile Biometrics’ Potential

Despite consumer demand for biometrics in banking and payments, as well as the banking sector’s push for mobile biometrics to unlock opportunities in digital channels, barriers to implementation and adoption remain. We have summarised the key results from the Oxford/Mastercard study which showed that there are discrepancies in the opinions of different stakeholders regarding various aspects of biometric systems.

A fundamental finding in the report is a knowledge gap among industry professionals who expect to be called upon to make critical implementation decisions. This paper guides these decision-makers through a simple framework of the often understated but critical criteria to ensure a holistic approach to implementing successful solutions in a dynamically changing technology and regulatory landscape.

With the Oxford/Mastercard report’s ‘Five Factor Framework’ as a base, we encourage industry professionals to refer to the key themes and critical criteria contained in this paper towards more effective collaboration in dealing with the implementation and operational complexities of mobile biometrics in financial services.
Sources:


**Mastercard** is a provider of primary and secondary research and analysis contained in this report and has supported its publication.

The Mastercard and University of Oxford study, “Mobile Biometrics in Financial Services: A Five Factor Framework,” can be found at https://www.cs.ox.ac.uk/research/publications/.

---

About Opus Research

Founded in 1986, Opus Research is a global provider of analysis and marketing strategy surrounding “Conversational Commerce,” a term coined in 2011 to describe business opportunities that exist at the intersection of smart user interface, artificial intelligence and analytics and consumer-facing ID and verification technologies. (www.opusresearch.net)

**For sales inquires please e-mail info@opusresearch.net or call +1(415) 904-7666**

This report shall be used solely for internal information purposes. Reproduction of this report without prior written permission is forbidden. Access to this report is limited to the license terms agreed to originally and any changes must be agreed upon in writing. The information contained herein has been obtained from sources believe to be reliable. However, Opus Research, Inc. accepts no responsibility whatsoever for the content or legality of the report. Opus Research, Inc. disclaims all warranties as to the accuracy, completeness or adequacy of such information. Further, Opus Research, Inc. shall have no liability for errors, omissions or inadequacies in the information contained herein or interpretations thereof. The opinions expressed herein may not necessarily coincide with the opinions and viewpoints of Opus Research, Inc. and are subject to change without notice.

Published June 2017 © Opus Research, Inc. All rights reserved.