



mastercard.

/Administration
/Human Resources
/Finance
/Marketing
/Publicity
/Promotion
/Research
/Business
/Development
/Engineering
/Manufacturing
/Planning

ELECTRONICS

GY

A MASTERCARD MARKET INTELLIGENCE REPORT

Biometrics

Meeting the challenge of authentication and payments technology

Table of contents

- ➔ Executive summary: Perfect timing for biometrics
- ➔ State of the market
- ➔ Urgency: The biometrics imperative
- ➔ Opportunity: Replacing PINs and passwords for better CX, security
- ➔ Issues: Getting mobile biometrics right
- ➔ Putting the framework into action
- ➔ Outcomes: Biometrics in motion
- ➔ Key takeaways
- ➔ Conclusions: Eliminating the biometrics knowledge gap



Executive summary

Perfect timing for biometrics

As biometric technologies captivate consumer and corporate imaginations, the mobile world has moved toward finger scanning and iris/facial recognition. For financial institutions, advances in recognition arrive at the perfect time, with data breaches dominating the news and biometrics adoption increasing rapidly.

Consumer demand for new forms of convenience and security has been met with innovation in this space, making mobile biometrics an urgent security matter—and a critical step for the credit and banking customer experience (CX).

The following report will show the overall landscape for the short-term future of biometrics as well an innovative methodology for deploying them. Many of the findings presented are from the research collaboration by Mastercard and Oxford University, "Mobile Biometrics in Financial Services: A Five Factor Framework", undertaken to help financial firms advance biometrics adoption more quickly.

"Consumers are driving the trend toward a password-free future where digital identity is all about who we are, not what we remember."

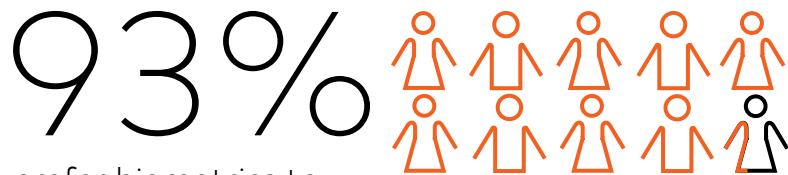
*Ajay Bhalla, president,
Mastercard Global
Enterprise Risk &
Security, June 2017*



State of the market

High demand for mobile biometrics

Consumers are excited and looking to adopt...



prefer biometrics to
passwords

...and banks are equally enthusiastic



want to adopt biometric
technology

Source: Oxford University Department of Computer Sciences and Mastercard,
Mobile Biometrics in Financial Services: A Five Factor Framework, 2017



Urgency: The biometrics imperative

Financial institutions playing catch-up

Even with the availability and maturity of mobile biometric solutions, financial industry adoption has been sporadic and inconsistent, and for good reason: As Mastercard executive VP for identity solutions Bob Reany told *Biometric Update* in June 2017, "there has been a lot of conflicting guidance about mobile biometrics coming from technology providers, industry influencers and the media." This is a challenge the industry needs to solve. As Reany points out, "we believe the potential of mobile biometrics in financial services is tremendous and will help us as an industry seamlessly blend optimal security with optimal customer experience, a critical win that has revolutionized other industries, like travel and media."

"Mobile Biometrics in Financial Services: A Five Factor Framework" from Oxford University Department of Computer Sciences and Mastercard contains these insights—including the fact that consumer adoption of biometrics is well ahead of financial institutions.

The report undertook exclusive research including a longitudinal (quantitative and qualitative) study with 449 end users of a deployed biometric recognition system in an online payments use case, investigating their perceptions before, during, and after having used a novel biometric system in a financial context for three months. It also included a targeted survey of financial services professionals primarily working in consumer banking. The result included a review of all scientific, industry and regulatory papers and standards to create a full overview and best practice guidance.



Biometrics knowledge gap in financial services

88%

of financial executives expect to be involved in a business decision regarding biometrics

36%

have experience with biometric technology

64%

of technical professionals claim to have little or no biometrics experience

Source: Oxford University Department of Computer Sciences and Mastercard, Mobile Biometrics in Financial Services: A Five Factor Framework, 2017

Opportunity

Replacing PINs and passwords for better CX and security

Ongoing data breaches of government agencies, credit bureaus, large retailers and other major organizations have thrown a spotlight on the weakness of forgotten or hacked PINs and passwords. Mobile biometrics now present a major opportunity for financial institutions to migrate away from less secure authentication, while improving CX (i.e., customer experience).



Static passwords

The bad...

- Increased complexity
- Regular changes required
- Easily guessable
- Brute force attacks easier

Consumers have up to **90 online accounts**

51%

of passwords used
at least twice

21%

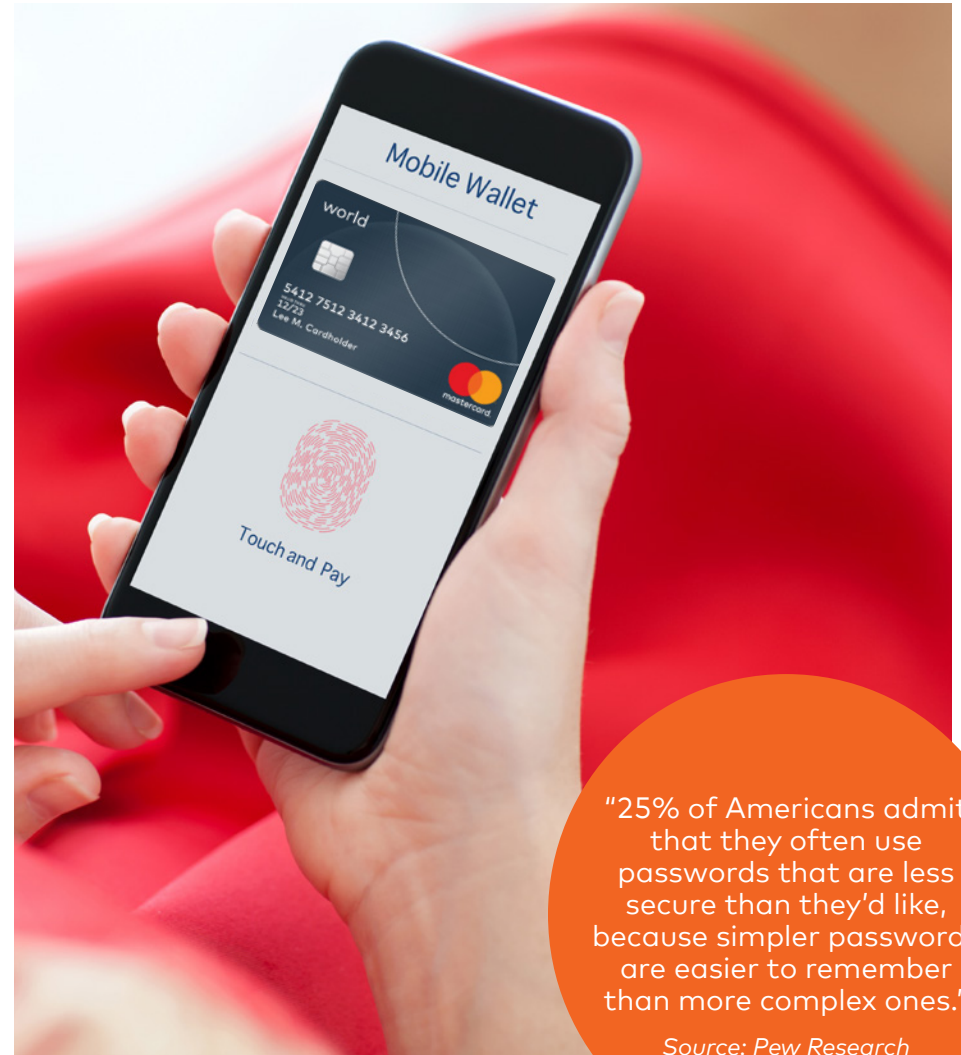
forget passwords
after 2 weeks

25%

of users forget at
least 1 password
per day

1/3 of online transactions abandoned at
checkout due to forgotten passwords

Source: Oxford University Department of Computer Sciences and Mastercard,
Mobile Biometrics in Financial Services: A Five Factor Framework, 2017



"25% of Americans admit that they often use passwords that are less secure than they'd like, because simpler passwords are easier to remember than more complex ones."

Source: Pew Research Center, 2017


Issues

Getting mobile biometrics right

Financial institutions may wish to consider a consistent enterprise to manage all touchpoints, as they may have disparate solutions in silos rather than a unified solution. Financial service executives will need guidelines in this regard to bring mobile biometrics to life.

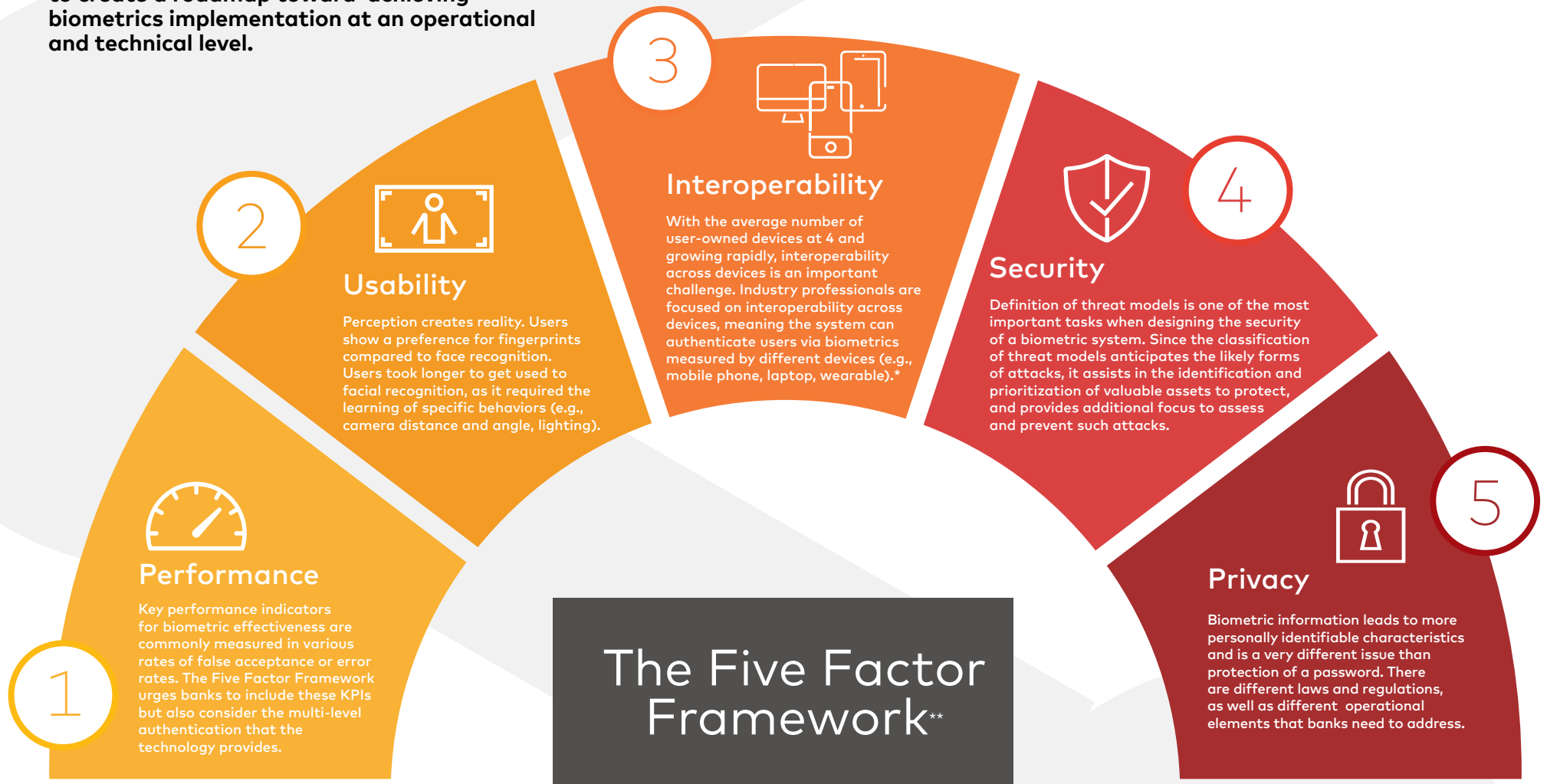
"The Five Factor Framework" helps to achieve a consistent enterprise solution by focusing on Performance, Usability, Interoperability, Security and Privacy. In addition to the full-length research report, we have captured insights in a succinct white paper to help executives understand and deploy biometric technology. Certain factors are more visible to the consumer, having a real impact on user experience, while others operate behind the scenes. Think of the framework as a checklist for financial service companies to reap the benefits of a cross-channel enterprise solution for ease of management and a more consistent consumer experience.

The Five Factor Framework

- 
- Performance**
1 Create frictionless, yet secure biometric solutions by combining low algorithmic error rates with a second factor of device ID for a multi-layered solution.
 - Usability**
2 Design a user experience that conveys trust and security while being easy enough to delight even the technophobes.
 - Interoperability**
3 Future-proof your solution to work with a range of devices, use cases and methods (face, iris, voice, etc.).
 - Security**
4 Minimize your risk by encrypting biometric templates and ensuring they never leave the user's device.
 - Privacy**
5 Use cutting edge protection technologies to preserve confidentiality and anonymity even within an authentication system.

Putting the framework into action

Financial institutions have an opportunity to create a roadmap toward achieving biometrics implementation at an operational and technical level.



Sources: *Digitas, Connected Commerce Survey, 2016

**Oxford University Department of Computer Sciences and Mastercard, Mobile Biometrics in Financial Services: A Five Factor Framework, 2017

Newsroom.Mastercard.com
@MastercardNews

Outcomes: Biometrics in motion

Many biometrics applications are already in place at many banks

Various biometric modalities such as fingerprint, facial, iris, etc. are currently in use across a variety of financial institutions across several markets.

Mastercard is focused on providing our partners with biometrics solutions ensuring consumer-centric over device-centric solutions.

More than

135 million people around the world

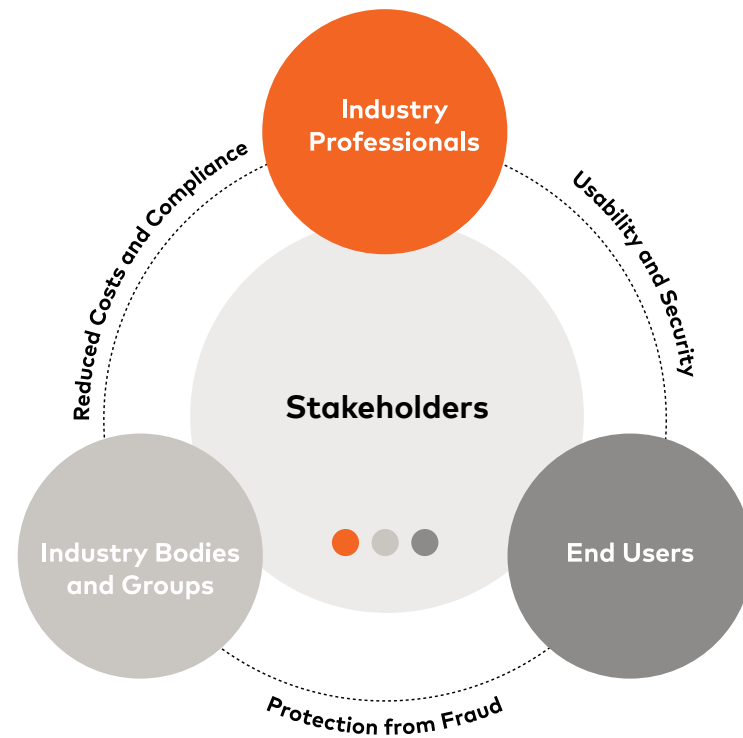
have enrolled for services that would use their voice to speed up the authentication process. Clients and customers of banks and financial service companies account for over half of this enrolled population.

The 135 million figure represents an

84% annual growth rate

during the two prior years. Banks saw a simultaneous increase in efficiencies through reduced call handling times, and even improved first call resolution with greater authentication successes.

Dimensions for successful mobile biometric implementations



Source: Opus Research Guidelines for Deploying Mobile Biometrics in Financial Services, 2017

Key takeaways

Professional and consumer momentum

The Mastercard/Oxford University survey measured perception of biometric technologies among consumers as well as financial industry professionals. Here are some detailed findings from that research:

Among industry professionals...



65%

believe users will adopt biometric solutions (face or fingerprint recognition)



67%

say multi-factor and multi-layer KPIs should be adopted



76%

believe biometrics are more secure than passwords



94%

believe users value convenience in authentication systems

Among consumers...

93%

state they will adopt biometric solutions

73%

believe biometrics will reduce fraud

83%

believe biometrics are more secure than passwords

92%

find biometrics more convenient than passwords

Conclusion

Eliminating the biometrics knowledge gap

There is a significant knowledge gap among financial executives regarding biometrics. That can be addressed with resources such as "The Five Factor Framework." A critical aspect is the need to apply biometrics enterprise-wide from banking login to authenticating payments to enabling transfers and even accessing call centers. Properly deployed, biometrics can make the CX more consistent and intuitive, and insights more valuable.

The future pace and quality of biometric adoption depends on three factors:



Consumer installed base: Mobile biometric capability is headed for 100% penetration.

The knowledge gap: 66% of companies plan to deploy a biometric system within 5 years. Yet, only 36% have any experience with implementing them.

Methodology: To ensure the best customer experience, banking executives need to focus on Performance, Usability, Interoperability, Security and Privacy.

Developing a Five Factor Framework





Further viewing and reading

As this report shows, biometrics is changing the way consumers see payments authentication. But financial service companies need to stay on the learning curve as biometrics evolves. Mastercard has created substantial content around the topic. We encourage you to watch the following videos on our Mastercard YouTube channel, and visit our white paper created with the University of Oxford.

The Truth About Mobile Biometrics: *Compromising Biometric Data*

<https://youtu.be/Rm2v4GPv8hA>

A deep dive into the technology behind fraud and how to protect consumer data with biometrics.

The Truth About Mobile Biometrics: *Differentiating Biometrics*

<https://youtu.be/GkO6N5kGbao>

The business case for investing in biometrics.

The Truth About Mobile Biometrics: *Spoofing Biometrics*

<https://youtu.be/2hooD5LvZto>

Learn how fraudsters try to "spoof" biometrics and the importance of judging the scale of fraud.

"Mobile Biometrics in Financial Services: A Five Factor Framework",

<https://newsroom.mastercard.com/news-briefs/overcoming-mobile-biometric-challenges-mastercard-and-university-of-oxford-collaborate-on-new-research-initiative/>

The definitive white paper on the future of biometrics.

A collaboration between Mastercard and the Oxford University



This document is proprietary to Mastercard and shall not be disclosed or passed on to any person or be reproduced, copied, distributed, referenced, disclosed, or published in whole or in part without the prior written consent of Mastercard. Any estimates, projections, and information contained herein have been obtained from public sources or are based upon estimates and projections and involve numerous and significant subjective determinations, and there is no assurance that such estimates and projections will be realized. No representation or warranty, express or implied, is made as to the accuracy and completeness of such information, and nothing contained herein is or shall be relied upon as a representation, whether as to the past, the present, or the future.