How mobile biometric authentication expands the reach of mobile banking

AWARE

AWARE

Table of Contents

The Mobile Banking Opportunity

For financial institutions, mobile banking is a cost-effective way to reach new consumers.
The technology offers financial inclusion and unprecedented convenience.

The Nielsen Mobile Shopping, Banking and Payment Survey **found 47 percent of consumers across the globe** used their mobile phones to check their account balances at least once in the six months prior to March 2016.

42 percent said they had used their mobile devices to pay bills. More plan to partake in such activities in the future.

Despite consumers' rising interest in mobile banking, onboarding and authentication obstacles hinder financial institutions' ability to position the technology as their primary customer engagement medium.

Biometrics technology offers the means to address these barriers.

What's Suppressing Mobile Adoption?

Of all the factors that affect consumers' willingness to use mobile banking applications, security, convenience, and user experience have the largest impact.

The Indian Institute of Technology found the majority of Indians choose whether to use mobile banking applications based on the technology's ease of use **(82 percent)** and ability to protect users' privacy **(86 percent).**

In the U.S., the Federal Reserve Board discovered that of those who did not use mobile banking, **88 percent said the technology couldn't meet their needs.** Many others **(80 percent)** said it was easier to pay with cash, debit or credit cards, and **42 percent** believe mobile banking apps don't adequately protect their information.

Greater access to mobile technology has not encouraged the majority of consumers to utilize mobile banking resources. **Much of this hesitancy is associated with authentication.**

Onboarding Challenges: Proving One's Identity

Nielsen discovered that mobile banking usage rates coincide with the percentage of the population living in rural areas. Places like China, India, Africa, and South America hold great promise for mobile banking.

Rural consumers represent a huge opportunity for banks, and financial institutions can leverage mobile banking to reach rural customers, extending their reach beyond physical geographic limitations. But engaging them relies on the use of mobile technologies for onboarding and authentication without sacrificing security.

Mobile onboarding introduces compliance requirements and a risk of fraud. For example, a fraudster could use a stolen identity to open a fake account in the victim's name. The process introduces customer due-diligence risk and regulatory compliance hurdles. This process is often referred to as "know your customer," or KYC, and can tend to inhibit a bank's ability to offer branchless banking services.

Authentication Challenges: Passwords

Most mobile banking applications use passwords to authenticate users.

But passwords provide inadequate security, and the need to remember and type them on a smartphone is terribly inconvenient for customers. Verizon's 2017 Data Breach Investigations report found **81 percent of data breaches** were a result of stolen or inadequate passwords. These credentials are based on what people know, and hackers can steal that knowledge through phishing, man-in-the-middle attacks, or other means.

Enter Password

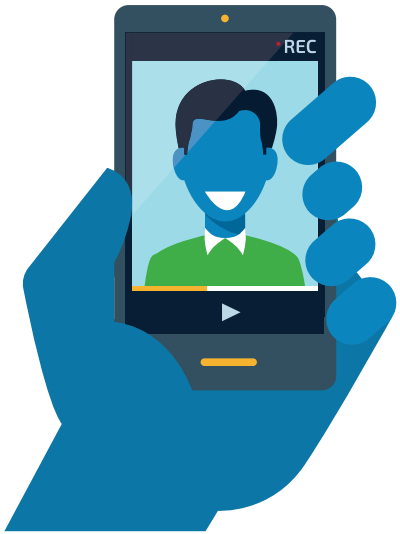
Sq3$g!5VH 2Rt1FE2u@ 900Ui!$#

*not strong enough

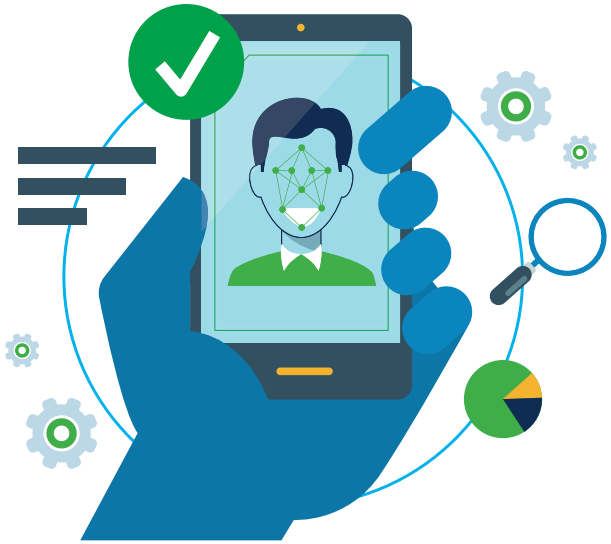
In addition, password requirements have become extraordinarily complex. Consumers have to remember long phrases consisting of both alphanumeric and non-alphanumeric characters. Also, the average person has **92 accounts registered to one email address,** according to Dashlane. To remember them, people tend to base their passwords on information that others can easily know, and use them across many accounts. So passwords are getting more complicated but not necessarily more secure.

How Facial Recognition Solves Authentication Challenges

Facial recognition improves login security by requiring the customer to match their live facial image with biometric data captured during enrollment.



Every time someone wants to log into his or her online bank account, he or she takes **a short live video of his or her face.**



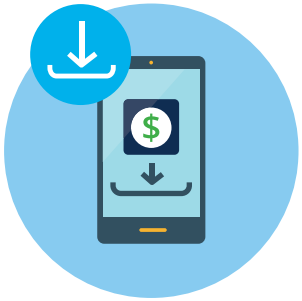
Algorithms are used to perform "spoof detection" and "liveness detection"; an analysis of the facial image to verify that it is a live image of the customer and not a fake image source such as a photo, video, or mask.

The live biometric is then compared to the stored biometric, and access is granted upon a positive comparison.

Biometrics and Mobile KYC

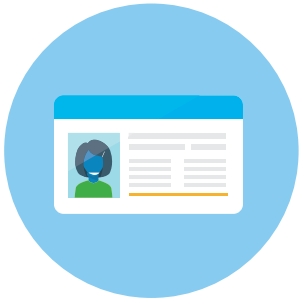
Facial recognition is emerging as a useful tool towards onboarding new customers and know-your-customer (KYC) processes. Biometrics allow new customers to enroll in banking services through their smartphones and avoid a branch visits, which is particularly convenient in rural areas. Here's one way the process can work:

1



A consumer downloads a bank's mobile app and selects an option **to register as a new customer.**

2



The app prompts the consumer to show **one or more forms of photo ID.**

3

After registering the ID documents, the app takes **a live image of the customer's face.**

4

Facial recognition software **matches the customer's live image to the photo ID.**

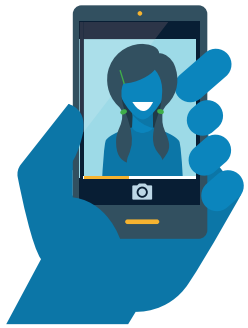
5

Technology can also be applied to verify the **authenticity of the ID.**

This biometric ID checking process is proving just as effective as if done by a bank employee.

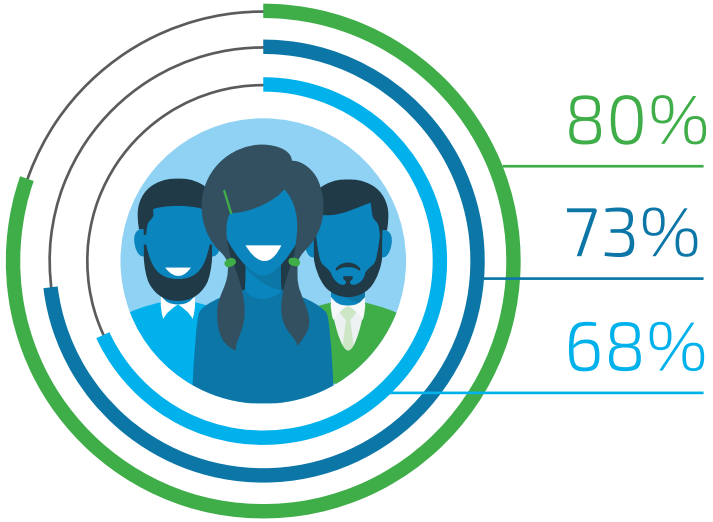
It is a convenient, secure way for customers to confirm their identities during the enrollment process without visiting branches. These facial images can be used for security functions in the future.

Increasing Customer Convenience



Opening accounts and authentication are areas where biometrics improve the security and convenience of mobile banking. In contrast to needing to remember a 12-character password and receiving verification codes via phone, customers can instead simply **take a selfie when they need to access online accounts.**

Consumers have expressed interest in using biometrics for authentication purposes. Gigya found **80 percent of consumers** believe biometric verification is more secure than methods involving usernames and passwords. Almost 50 percent of millennials already use some kind of biometric information to authenticate themselves. In addition, Aite Group found **73 percent of millennials and 68 percent of Gen Xers** believe facial recognition is an easy way to identify themselves. Even most baby boomers feel that facial recognition is a simple authentication option.



How can banks integrate facial recognition into their operations?
Are there cost-effective biometric solutions?

Increasing Customer Convenience

Biometrics as a Service (BaaS) is an increasingly viable way for institutions to leverage biometrics.
Instead of deploying software and storing biometric data, banks can use a subscription-based service to integrate biometric KYC and authentication capabilities into existing systems and processes.

BaaS platforms offer...

- **Enrollment**
- **Authentication**
- **Liveness detection functions**

...allowing banks to deliver convenient customer experiences while fulfilling KYC obligations.

If you want to learn more about how biometrics and BaaS can benefit your organization,
reach out to Aware for an in-depth discussion about their technology, products, and experiences.

AWARE

aware.com/contact

www.nielsen.com/us/en/insights/news/2016/digital-deposits-mobile-banking-around-the-world.html
www.icommercecentral.com/open-access/factors-affecting-mobile-banking-adoption-behavior-in-india.php?aid=70187
blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/
www.telesign.com/wp-content/uploads/2016/11/TeleSign-Consumer-Account-Security-Report-2016-FINAL.pdf
www.gigya.com/survey-reveals-52-percent-of-consumers-want-biometrics/
Aite Group: drive.google.com/a/brafton.com/file/d/0B9BVKdLhNKofVndUNTZOaVNXekk/view?usp=sharing