White Paper

Branchless Banking with Biometrics

AWARE

781.276.4000 | sales@aware.com | www.aware.com

Aware is a leading global provider of software products and solutions for biometric identification and authentication. They are used for variety of applications including financial services, enterprise security, border management, and law enforcement. Aware is a publicly held company (NASDAQ: AWRE) based in Bedford, Massachusetts.

The world has truly gone digital. It is currently estimated that 3.8 billion people own a smartphone[1], representing almost half of the entire world's population. The rapid ascendance of smartphones around the world in recent years has upturned much of how we live our lives, from social media to online shopping. Banks and financial services companies have also had to adapt to this new digital landscape, providing their customers with new ways to access and manage their accounts.

The arrival of COVID-19 only escalated these trends, greatly increasing overall demand for mobile-based financial solutions that wouldn't require in-person visits that could jeopardize one's health. This combination of smartphone ubiquity and reluctance to travel has shone a spotlight on traditional financial onboarding and authentication procedures, highlighting just how important it is to provide financial customers with a means to both open and access their accounts securely from a remote location. With so many banks and financial companies looking for ways to address these challenges, biometrics are an ideal solution for secure, remote onboarding and transaction authentication.

The Mobile Banking Opportunity

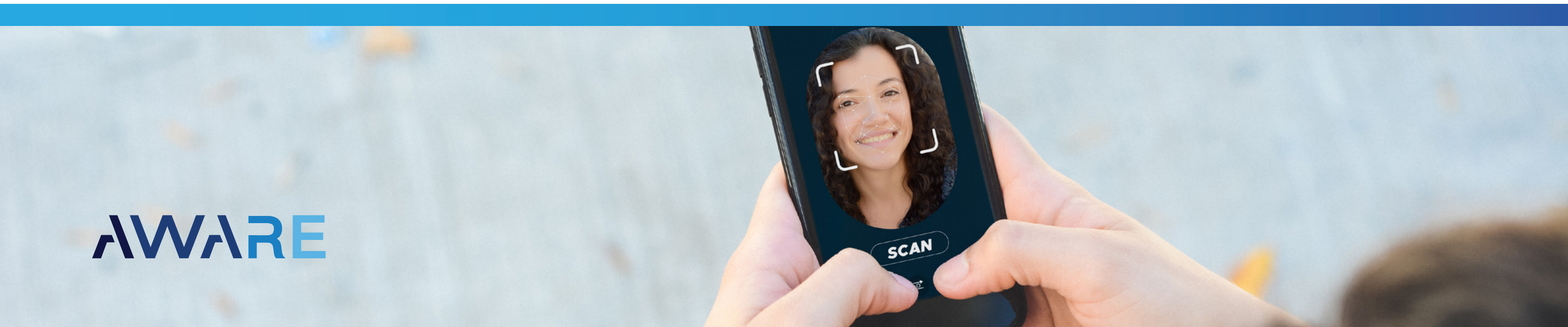
For financial institutions, mobile banking has become a cost-effective way to reach new customers. The technology permits customer access to financial accounts from virtually anywhere in the world, real-time financial transactions without visiting a branch, and unprecedented convenience overall. Customers have responded well to mobile solutions as well, with 47 percent of consumers across the globe using their mobile phones to check their account balances at least once in the last six months[2]. Mobile banking appears poised to stay too, with 42 percent of consumers saying that they have not only used their mobile devices to pay their bills in the past, but plan to continue to do so in the future[3].

Despite the positive reaction from consumers, and their ongoing rising interest in the technology, financial institutions have thus far had difficulty positioning mobile banking technology as their primary means of customer engagement. This is largely due to the many challenges they face from contemporary mobile onboarding and authentication procedures.

Traditional Financial Onboarding and Authentication

Two key workflows for any banking or financial account customer are onboarding and transaction processing. Onboarding is the process through which individuals start their journey as a customer, and is typically the point upon which they open a new account. Transactions, subsequently, typically constitute any time a customer needs to access their personal account to move money or make a change.

Historically both onboarding and account access have been in-person processes, requiring an account holder to visit a local branch. The representative at the branch would then verify the person's identity face-to-face and handle the customer's specified needs. With the proliferation of the internet and smartphones, these in-person requirements began to shift to more mobile solutions that could be performed online. Today, most financial institutions provide their customers with a means to perform transactions online or from a mobile device.



The onboarding process, however, still primarily remains an in-person procedure. This is primarily due to the fact that onboarding is largely an identity verification process. For financial institutions in particular, knowing your customer is critical to ensuring their valuable assets, and subsequent account access procedures, are safe and secure. Unfortunately, this in-person requirement is increasingly inconvenient for customers.

Examples of Fraud

Banks are familiar with the many ways that fraudsters can attempt to steal from them and their customers; among them are "presentation attacks" that attempt to defeat biometric security mechanisms. In some of the most common cases, fraud is perpetrated not by strangers but by family members or even employees. Career fraudsters tend to rely on techniques that are more repeatable. In both cases, biometrics make onboarding and authentication more resilient to fraud, but require liveness detection to do so. Following are some examples of presentation attacks and the role of liveness detection.

Insider Attacks

A common category of fraud is committed by a known party; a family member, friend, or co-worker with relatively easy access to identity data of their unsuspecting target. They attempt to use it to impersonate their victim to either open a new account in their name or to access their existing account without their knowledge. Using facial recognition makes these types of attack much more difficult; adding voice biometrics, even more so. In either case, liveness detection is necessary to prevent the perpetrator from using a photo or video of their victim—a "spoof"—to impersonate them.

A less common category of insider fraud is perpetrated by bank employees. Here, an employee collects identity data from an account applicant as part of their onboarding process but then also takes a photo or video of them using their personal mobile device. The applicant doesn't recognize that this is not part of the standard process. The employee then uses the account information and customer's facial image to access the new account; the customer's credit line is gone before they ever get to use it. Liveness detection prevents this type of insider attack.

Synthetic Identities

Yet another category of fraud involves the creation of "synthetic identities" that are created and used by fraudsters to get credit and loans that they never plan to pay back. They can do this over and over by using sets of identity information that are either completely fictional or base partly on a real person. Facial biometrics can be used to help secure a mobile onboarding process against the use of synthetic identities. But without liveness detection, a fraudster could use a photo or video of someone else, or a selfie in which their face is partially obscured. This prevents the image from being used for several useful biometric onboarding mechanisms.

The Challenges of Contemporary Onboarding

While in-person onboarding is certainly a tried-and-true method of customer registration, there are a number of challenges to current procedures that financial institutions are increasingly forced to address. The first is **inconvenience**. With nearly half of the earth's population now accustomed to conducting their business from their smartphones, requiring customers to visit an office is an increasingly outdated notion. Customers already expect to be able to pay their bills and scan checks via their smartphones, so having to visit a branch to open an account often comes as an inconvenient surprise. COVID-19 has only exacerbated this problem, forcing people to rely on mobile devices more than ever before.

Today's onboarding experiences are also **time-consuming**. Putting travel time to the side, waiting for a representative, processing paperwork and verifying identification documents is a long process for customers to endure. Approximately 63% of consumers have abandoned an application because of how long the process took[4], representing a potentially major problem for financial institutions.

Another major challenge for contemporary onboarding procedures is how it limits an institution's ability to **attract new customers**. Rural populations represent a huge opportunity for banks, but these customers do not always have reasonable access to a local branch or office. This lack of access limits the ability of banks or financial services companies to bring on new clients. Providing a secure, mobile onboarding process would not only be more convenient for existing customers, but it would also help bring on new ones too.

Lastly, 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.

The Challenges of Contemporary Authentication

When it comes to mobile banking applications, most use passwords to authenticate users and grant access to their accounts. Unfortunately, passwords are no longer a satisfactorily secure authentication method, as evidenced by the near daily reports of new instances of large-scale data breaches or widespread fraud. In 2017, it was found that 81 percent of all data breaches were a result of stolen or inadequate passwords[5]. These credentials are based on what people know, and hackers can steal that knowledge through phishing, man-in-the-middle attacks, or other means.

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[6]. To remember them, people tend to base their passwords on information that others can easily know, and use them across many accounts. So while passwords are getting more complicated, they are not necessarily more secure.

The cost of cyberattacks has hit the banking industry the hardest in recent years, reaching an average cost of $18.3 million annually per company[7]. It is currently estimated that over 70% of all data breaches are financially motivated[8], putting increasing pressure on banks and financial companies to take measures to prevent these types of attacks from being successful. The simple fact is that passwords are no longer secure enough to protect our financial assets and personal information. To both combat these threats and address today's onboarding challenges, biometrics are an ideal solution to consider.

The Benefits of Biometrics in Financial Onboarding and Authentication

There are a number of reasons why biometrics should be a top consideration for banks and financial institutions looking to improve their onboarding workflows and protect their valuable assets:

Mobile-Based:

Facial and speaker (voice) recognition is emerging as a useful tool towards onboarding new customers and know-your-customer (KYC) processes. Modern day biometrics are increasingly mobile, allowing new customers to enroll in banking services through their smartphones and avoid a branch visit, which is particularly convenient in rural areas.

Today's biometric solutions use the cameras and microphones found in today's smartphones and mobile devices to perform highly accurate face and voice recognition. Identification documents such as driver's licenses or passports can also be matched to an individual and verified through the use of "selfies" and mobile biometric functionality. By putting this functionality in the hands of the consumer, they can be registered into a system or subsequently authenticated from virtually anywhere, increasing a company's ability to conveniently service their existing clients and attract new ones currently unwilling or unable to visit a local branch.

Overall, this mobile biometric process is proving to be just as effective as if done by a bank employee. It is a convenient, secure way for customers to confirm their identities without visiting branches. And the facial images or voice samples can be used for security functions in the future.

Increased Security:

With passwords increasingly shown as an unreliable authentication method, biometrics serve as an ideal alternative for those looking to increase security. Facial and speaker recognition improve login security by requiring the customer to match their live facial image or voice sample with biometric data captured during enrollment. The live biometric is then compared to the stored biometric, and access is granted upon a positive comparison.

One key advantage is that unlike passwords, biometrics cannot be stolen or guessed at. Biometrics use something that is unique to each person—a face or voice—making it much more difficult for would-be attackers to bypass. Biometrics also commonly feature algorithms that perform liveness detection to determine whether a user is a living, breathing person, and not a presentation or "spoof" attack using a photo, video or mask.

With such biometric measures in place, banks and financial companies can be sure that the customers being onboarded are not impostors looking to open an account fraudulently, and that their customer authentication procedures are no longer susceptible to fraud-prone passwords.

Added 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.

The inclusion of biometrics adds a level of convenience to nearly every customer interaction. By being mobile, customers no longer need to travel to a local branch to open an account or process a transaction. Mobile biometrics are also fast, performing a face and voice match with liveness detection in seconds. The process is a frictionless one for users too, requiring no additional steps beyond a selfie and/or voice prompt. Lastly, many biometric solutions have flexible configurations to choose from, placing the functionality on the device or server to address varying network availability and providing customers with a biometric solution virtually anywhere in the world.

Consumers have expressed interest in using biometrics for authentication purposes as well. Approximately 80 percent of consumers believe biometric verification is more secure than methods involving usernames and passwords[9]. Almost 50 percent of millennials already use some kind of biometric information to authenticate themselves. Even most baby boomers feel that facial recognition is a simple authentication option.

Providing Secure, Convenient Onboarding and Authentication with Knomi®

The Knomi® mobile biometric authentication platform is a strong option for any bank or financial services company looking to improve their onboarding or authentication practices to address today's challenges. Knomi uses mobile devices to provide secure and convenient facial and voice recognition for mobile multifactor authentication.

Mobile Onboarding:

Knomi provides identity proofing to support mobile onboarding. Advanced security checks can authenticate driver's licenses and passports, and ensure spoof-resistant biometric facial matching between live and printed images. Knomi onboarding includes biometric facial matching to identification documents, and verification for over 9,000 documents worldwide. Knomi liveness detection also detects impostors, preventing them from opening accounts fraudulently.

Mobile Authentication:

Knomi provides password-free multifactor authentication using facial and voice biometric recognition and liveness detection, and is based on NIST-tested face and voice matching algorithms. With Knomi's multimodal biometric capabilities, users can be authenticated with their faces, voices, or a combination of the two for even higher security. Knomi can also be configured for many different use cases, providing banks and financial institutions with the means to customize the customer experience for whatever the need.

Liveness Detection:

Knomi's advanced presentation attack detection algorithms detect not only victim impersonation, but also identity concealment, providing banks and financial companies with the peace of mind that their customers are who they say they are. Knomi liveness detection is also passive for users, requiring no additional steps (such as prompted head movements) to be effective. And Knomi liveness works for onboarding, authentication, and document verification workflows as well.

Flexible Configurations:

Besides supporting a full range of mobile and server-based operating systems, the Knomi platform is available in device-centric, server-centric, and browser-based configurations. Device-based configurations place the biometric functionality onto a person's device and are ideal for situations where network availability is not guaranteed. Server-based configurations, however, place the biometric functionality on the server; a perfect solution for when network availability is strong. Knomi's browser-based configurations serve as a third option, performing biometric capture directly through a browser, and placing additional functionality on the server. Whatever the choice, Knomi will continue to provide the same level of security and convenience.

How Latin American banks use Knomi to enable secure, low-friction onboarding

New customers are a critical source of any bank's revenue growth, so onboarding them efficiently is among the most important functions they can perform. But onboarding is also a time when banks are most vulnerable to fraud. Onboarding is largely an exercise in identity verification, where the bank attempts to gauge whether a potential account holder can be trusted with a line of credit and will behave as a customer in good faith.

Banks that have incorporated Knomi software into their onboarding process can leverage an applicant's live selfie to conduct several identity checks that serve to positively verify their identify and to detect when fraud is being attempted.

Different versions of Knomi allow the process to be conducted either from the bank's mobile app or alternatively via a web page on a mobile device or desktop. A URL can be discovered by the applicant on the bank's website, advertisement email, or banner ad. A potential customer simply clicks on the link from their mobile or desktop to initiate an application process in a browser, which includes capture of a live selfie. In this way, a biometrics-enhanced, browser-based process and simultaneously increase the security and reduce the friction of an onboarding process that doesn't require an applicant to install a mobile app before applying.

Latin American banks are using Knomi facial recognition and liveness detection to conduct several different identity verification and fraud detection checks upon onboarding. Liveness detection alone serves several valuable purposes:

- **Detection of attempted impersonations of a targeted victim** using "spoofs" such as paper or digital photos, videos, or 2D and 3D masks;
- **Detection of attempted identity concealment using a non-self**, non-human, or partially obscured facial image to avoid future facial recognition-based search detection; and
- **Non-repudiation,** which is a term to describe a bank's ability to collect court-admissible evidence that associates the activity of a fraudster to a real person; that is, prevent the fraudster from repudiating his involvement in a fraud attempt.

But liveness detection is also an essential part of these other security measures that rely on biometric matching and search, which are each being employed by one or more of Aware's Latin American customers as part of an onboarding process:

- **Facial image match-to-ID.** This function, along with liveness detection, ensures that the government-issued identity document used to convey identity data is authentic and belongs to the applicant.
- **Duplicate checks.** Facial images of other customers are searched to ensure that the applicant is not attempting to surreptitiously hold multiple accounts, use a synthetic identity, or assume the identity of an existing account holder.
- **Watch list checks.** Databases of facial images of known fraudsters are searched to ensure that the applicant is not a known fraudster.
- **External bureau checks.** Facial images can be submitted to external law enforcement bureaus to determine whether they have a criminal history.

An Example of the Mobile KYC Process

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.

The Future of Mobile Banking Lies With Biometrics

Consumers' expectations of their mobile banking apps continue to rise, particularly as we go cashless. They expect to be able to access their accounts and process transactions virtually anywhere, without compromising security. Because they are inherently more secure, convenient and flexible than contemporary alternatives, today's biometric solutions provide financial companies with a powerful and elegant identity verification approach to meet today's customer needs and expectations.

With increased travel hesitancy stemming from COVID-19, and rising rates of identity theft and data breaches around the world, now is the ideal time for banks and financial institutions to consider addressing these challenges by upgrading their onboarding and authentication procedures with biometric technology. By both protecting their existing customers, and attracting new ones as well, banks and other institutions are increasingly viewing biometrics not only as a business imperative, but a future reality.

For more information about the Knomi mobile biometric authentication platform, please contact us or visit our webpage.

Interested in learning more about Knomi? Visit www.aware.com/knomi/

Sources:

1 - www.bankmycell.com/blog/how-many-phones-are-in-the-world
2 - www.nielsen.com/us/en/insights/news/2016/digital-deposits-mobile-banking-around-the-world.html
3 - www.nielsen.com/us/en/insights/news/2016/digital-deposits-mobile-banking-around-the-world.html
4 - www.signicat.com/battle-to-onboard
5 - www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/ 6
6 - blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/
7 - www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
8 - www.verizon.com/business/resources/reports/dbir/
9 - www.gigya.com/survey-reveals-52-percent-of-consumers-want-biometrics/