White Paper

Improving Financial Onboarding and Authentication Through 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.

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—an increasingly inconvenient requirement for customers.

The Challenges of Contemporary Practices

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[2], representing a potentially major problem for financial institutions.

The last major challenge for contemporary onboarding procedures is how it limits an institution's ability to

attract new customers. Rural populations 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.

When it comes to transaction processing, today's banks and financial institutions already provide their customers with the ability to process transactions via a mobile device. But while that satisfies many of the problems faced by contemporary onboarding, there is an underlying problem with modern authentication procedures: passwords are no longer a satisfactorily secure authentication method. Every day it seems like we hear of new instances of large-scale data breaches or widespread fraud, as hackers have gotten quite adept at stealing or guessing-at passwords.

The cost of cyberattacks has hit the banking industry the hardest in recent years, reaching an average cost of $18.3 million annually per company2. It is currently estimated that over 70% of all data breaches are financially motivated[3], 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:

Modern day biometrics are increasingly mobile, using 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.

Increased Security:

With passwords increasingly shown as an unreliable authentication method, biometrics serve as an ideal alternative for those looking to increase security. 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 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:

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.

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 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.

With increased travel hesitancy and rates of identity theft and data breaches, this is an ideal time for banks and financial institutions to consider upgrading their onboarding and authentication procedures. Thanks to the added security, convenience and flexibility they provide, today's biometric solutions provide financial companies with a way to not only protect their existing customers, but attract new ones as well.

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

Sources:
1 - https://www.bankmycell.com/blog/how-many-phones-are-in-the-world
2 - https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
3 - https://www.verizon.com/business/resources/reports/dbir/

AWARE