White Paper

Improve Digital Onboarding Solutions with Biometrics

AWARE

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

Aware, Inc., (NASDAQ: AWRE) is a leading authentication company applying proven and trusted adaptive authentication to solve everyday business challenges with biometrics. Aware's software and software-as-a-service offerings address the growing challenges that government and commercial enterprises face in knowing, authenticating and securing individuals through frictionless and highly secure user experiences.

Prior to the lockdown, companies were already looking to improve convenience for? their customers by giving them the option of digital onboarding. However, the COVID-19 pandemic created even more dependency on remote onboarding and mobile devices, increasing consumer demand for better digital onboarding solutions. To stay competitive in this environment, many businesses have had to adopt new strategies and practices. With increased consumer demand comes the need to ensure that the onboarding process can perform as a stand-alone function. Now more than ever, businesses need to enroll customer identities accurately and securely, without allowing malicious actors to impersonate others and establish fraudulent accounts.

Digital onboarding defined

Customer onboarding is a critical process for establishing a new customer relationship. Onboarding is the process of acquiring or subscribing new users, ensuring that they have access to all the services and products that an organization – simply and efficiently., integrating them into the database. In fact, the onboarding process is the official beginning of a customer-client relationship as an individual becomes a registered user or official client. Although the concept of onboarding is well known in the field of human resources and talent management, this term is widely used in any field in which an organization needs to incorporate a person into its structure, either as a client, as an employee or as a user. In the financial and banking sector, the onboarding process is referred to as KYC or "know your customer". The practice is carried out by companies who need to verify the identity of their clients with full compliance, following legal regulations and requirements.

Digital onboarding is the digitized version of standard onboarding procedure. It is conducted completely online and remotely from any device with the ability to capture biometric modalities (i.e face, fingerprint, iris or voice recognition), eliminating the need for the customer to visit an office, along with bringing a number of documents to validate their identity. This has made onboarding and KYC procedure convenient, fast, and easy. Current approaches are mostly reliant on customer inputs, background checks and ID/document verification alone. While some providers have begun utilizing "selfies" and video to confirm/enroll user identities, there is always the risk of identity impersonation, and without a higher level of security, threats will remain.

Challenges with current digital onboarding methods

The acceleration and adoption to digital solutions has caused an increase in fraud occurrences and the cost associated with fraud. On average, according to Experian[1], 1 in 20 Americans are victims of identity theft every year. In 2019, 13 million American consumers were affected, resulting in a total fraud loss of an estimated $17 billion. Unfortunately, there has also been a 53% increase in identity theft from 2019 to 2020 and fraud numbers continue to rise:

- **Consumers filed 2.2 million[2] fraud reports in 2020.**
- **47% of Americans[3] experienced financial identity theft in 2020.**
- **9 in 10 Americans[4] encountered a fraud attempt in the past year.**
- **33 million (1 in 6)[4] Americans lost money to identity theft last year.**
- **Consumers lost more than $56 billion[5] to identity theft and fraud in 2020.**

The COVID-19 pandemic had an enormous impact on fraud and identity theft. During these unprecedented times, there was an uptick in fraud related calls, letters and emails from scammers posing as the IRS. As a result, consumers have reported a losing more than $588 million[6] to COVID related fraud since the beginning of 2020 according to the Federal Trade Commission. March 2021 TransUnion[7] analysis showed that 36% of consumers who said they are being targeted by digital fraud related to COVID-19 in the last three months is higher than approximately one year ago. In April 2020, 29% said they had been targeted by digital fraud related to COVID-19. In the U.S., this percentage increased from 26% to 38% in the same timeframe.

As a result, customers today are becoming more concerned about the security of the accounts they use. In addition, these customers are demanding a frictionless user experience. Pre-pandemic, consumers accepted poor digital experience, but this is no longer the case. According to Signicat's report[8] almost two in three people who begin a digital application do not complete it. It means an increase of 23 % in abandonment rates since the first report was published in 2016. Poor onboarding damages brand reputation. More than half of all customers are less likely to use the brand in the future, and a third will advise friends against doing the same. Data collected from the Signicat's report also highlighted that:

- **~25% of customers consider the onboarding process too difficult**
- **1 in 5 users abandoned the process because it dragged on too long**

Biometric technology holds the key

A recent report from Onfido's 2022 Identity Fraud Report[8] found that selfie-based biometric authentication is highly effective against identity fraud. According to Onfido[9], the average document fraud rate over the first nine months of 2021 was 5.9%, whereas the fraud rate for selfie-based identification systems was only 1.53%. Video selfies, meanwhile, brought the fraud rate down to just 0.17%.

Selfie based identification or facial recognition[10] is becoming vastly popular amongst consumer products. Facial recognition technology applies the science of biometrics to a user's facial features. Facial recognition algorithms create a biometric template by detecting and measuring various characteristics, or feature points, of human faces, including location of the eyes, eyebrows, nose, mouth, chin, and ears. Templates are compared to yield a match score, which indicates the likelihood that the images belong to the same person. Liveness detection may also be applied to ensure that the source of the biometric sample is not a digital or paper reproduction.

In addition to consumer demand, there are several reasons why biometrics should be a top consideration for businesses hoping to improve their digital onboarding process 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 using "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 these biometric measures, 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 can say bye to in-person onboarding measures. 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.

Provide secure, convenient onboarding with Knomi®

The Knomi® mobile biometric authentication platform is a strong option for organizations or even individuals looking to improve their onboarding or authentication practices. With Knomi, organizations can improve user experience and combat high fraud rates. 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.

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

Sources:

1 https://www.experian.com/blogs/ask-experian/how-common-is-identity-theft/

2 https://nam10.safelinks.protection.outlook.com/GetUrlReputation

3 https://giact.com/identity/us-identity-theft-the-stark-reality-report/

4 https://www.aarp.org/research/topics/economics/info-2021/fraud-victim-susceptibility-study.html

5 https://www.javelinstrategy.com/press-release/total-identity-fraud-losses-soar-56-billion-2020

6 https://public.tableau.com/app/profile/federal.trade.commission/viz/COVID-19andStimulusReports/Map

7 https://newsroom.transunion.com/one-year-after-covid-19-new-transunion-research-shows—digital-fraud-attempts-against-businesses-have-increased-by-46/

8 https://onfido.com/landing/identity-fraud-report/

9 https://findbiometrics.com/biometric-security-significantly-reduces-id-fraud-suggests-onfido-report-7122103/

10 https://www.aware.com/lp/facial-recognition/