Case Study

Mobile Biometrics and Liveness Detection

How Latin American banks are using Knomi™ to win more customers and prevent fraud

AWARE

Introduction

> For Aware's banking customers in the region, biometrics — and facial recognition in particular—are playing a big part in making mobile banking more accessible by making it more convenient and secure.

Dramatic advances in mobile phone technology and networks present banks the opportunity to make their services more accessible. Customers can now use their mobile devices to quickly apply for new accounts and credit lines, access their account information, and perform purchases and transactions, all without ever visiting a branch or ATM. Credit towards purchase of big-ticket items such as home appliances, electronics, and furniture can be issued on the spot by retailers at the point of purchase.

By many measures, Latin America leads the world in adoption of biometrics for commercial applications, and financial services companies are a major contributor to the trend. For Aware's banking customers in the region, biometrics—and facial recognition in particular—are playing a big part in making mobile banking more accessible by making it more convenient and secure.

In every case, the banks are using "liveness detection" offered as part of Aware's Knomi™ mobile biometric authentication solution. Liveness detection is used to ensure that the facial images being collected can be trusted for a variety of biometrics-based security checks. It's applied during onboarding of new customers as well as for enhanced login to mobile apps using biometric authentication.

Examples of fraud prevented by facial recognition and liveness detection

Banks in Latin America are all too 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 and 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 based 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 be used for several useful biometric onboarding security mechanisms (see below).

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 identity and to detect when fraud is being attempted.

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.

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 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 can 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.

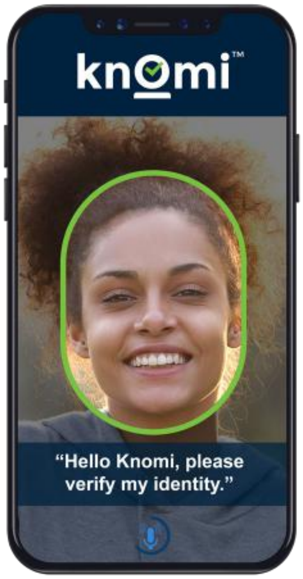
But liveness detection is also an essential part of these other security measures that rely on biometric matching and search, which are each being employed by one or more of Aware's Latin American customers as part of an onboarding process:

- **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 the 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.

Mobile authentication using trusted biometrics from onboarding

Once customers are onboarded and have opened an account, banks can now use the selfie captured during the enrollment process to enable them to more securely and conveniently log into their account and conduct transactions through their mobile app. Aware's Latin American customers have incorporated biometric authentication into their mobile banking apps, where it is used either as an alternative to passwords, or as a step required in addition to passwords for higher-value transactions.

As with onboarding, liveness detection is an essential function for mobile biometric authentication, since without it, a fraudster with access to their victim's phone could otherwise use a spoof to impersonate the device owner and access their accounts. Liveness detection prevents this presentation attack.



Yet another way to make biometric authentication even more resistant to spoofing is by employing a multimodal approach; that is, requiring a biometric modality in addition to face such as voice. This improves the biometric security (fewer false matches) and convenience (fewer false non-matches) performance by an order of magnitude.

But adding voice matching and liveness detection also makes the task of spoofing exponentially more complicated. Voice liveness detection utilizes algorithms that detect whether a voice sample has been previously recorded or has been generated synthetically. With a face-only approach, the fraudster needs a successful face spoof to defeat the biometric security. With face and voice together, the fraudster also needs to successfully match and spoof the victim's voice, which is particularly difficult, in part because voice samples of victims that could potentially be used to create a spoof are much more difficult to come by. In short, multimodal biometrics have an exponential effect on performance and security, which is particularly useful for high-value transactions.

Adding voice matching and liveness detection also makes the task of spoofing exponentially more complicated.

Biometrics are becoming an essential part of mobile banking

Consumers' expectations of their mobile banking apps continue to rise, particularly as we go cashless. Yet there are no expectations that this ability should come with any sacrifice in security whatsoever. Identity is a foundational element of banking, and biometrics are a powerful and elegant identity verification approach that is complementary to other security mechanisms. Biometrics also happen to offer a level of convenience that consumers have come to demand. For several banks in Latin America, biometrics are a business imperative. Their vision is one of biometrics as an essential feature of their services and brand. With Knomi, Aware is helping them make that vision a reality.

AWARE
www.aware.com/contact