White Paper

Easy But Strong:

How Financial Services Companies Can Benefit from Biometric-backed Security

AWARE

781.687.0300 | 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 Burlington, Massachusetts.

It's hard to beat the convenience of "online." Movies from the comfort of recliners, sporting events with endless snacks nearby in the kitchen, or grocery selection and delivery without leaving the sofa – it's expected that all things be made available through connected devices. It is estimated that 3.8 billion people own a smartphone[1], representing almost half of the world's population.

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. From the customer's view, it's hard to beat the convenience of depositing checks, checking statements, and moving money anytime or anywhere we choose. The COVID-19 pandemic only escalated an already rising trend, further increasing the demand for mobile-based financial solutions that wouldn't require in-person visits. The number of active online banking users worldwide is expected to grow to more than 2.5 billion by 2024, up from 2.1 billion today.[2]

This combination of smartphone ubiquity and the desire for convenience 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.

However, those in financial services know that this is no small task. There's no shortage of bad actors out there. What's more, financial institutions also face stringent regulatory oversight as part of anti-money laundering (AML) policies, which means it's critically important for banks to establish the legitimacy of a customer's identity. Regulatory authorities aren't the only ones requiring security; customers also expect it.

Some Challenges That Financial Institutions Face Today

Banks are familiar with the many ways fraudsters can attempt to steal from them and their customers; among them are "presentation attacks" that attempt to defeat biometric security mechanisms. Unfortunately, the attempts don't stop there. Hackers are increasingly known to create entirely falsified identities to circumvent more traditional security measures in financial services. If that's not enough, synthetic videos and imagery are within reach of even the most casual green hat hacker.

Synthetic Identities

A stolen identity is one that has been misappropriated from someone – either online or offline – so that a criminal can commit fraud in the owner's name. The identity thief might have gotten personally identifiable information (PII) through a data breach, a "phishing" scam, spyware, public wi-fi intrusion, stolen property, or many other ways. The result, however, is typically the same. Criminals use their stolen identity to open additional credit, get loans, or go on a spending spree.

Synthetic identity fraud is a more nuanced approach to theft. Synthetic identities are real and valid identities created by criminals using fabricated credentials. Think of it as assembling the pieces of a puzzle. Each piece of the puzzle is stolen or forged but then assembled into something that has been legitimized. The process isn't often fast. A criminal can take weeks to build a synthetic identity and then months or longer to legitimize the identity after it is

created. But what it lacks in speed, it makes up for in imperceptibility – an attractive attribute for those looking not to get caught.

Older adults are sometimes less comfortable with technology and more trusting of individuals and are common victims. And children, whose credit history is typically "clean" and not usually monitored, can also be prime targets. More than 1.25 million children were victims of identity theft in 2021, according to a study done by Javelin Strategy & Research.[3]

Facial biometrics can be used to help secure a mobile onboarding process against the use of synthetic identities. But without liveness detection – a process that determines whether a user is a living person and not a mask or similar presentation attack - a fraudster could use a photo or video of someone else or a selfie in which their face is partially obscured, making liveness detection a key component of securing financial institutions' onboarding and authorization processes.

Deepfakes

If you've spent time on social media, you might have come across what is a potentially concerning technological advancement – the deepfake. Deepfake images can be seen as anything from entertaining to concerning – or even scary. A political figure spreading propaganda they didn't truly spread. A historical figure making a speech they didn't actually make. A famous actor doing or saying things they didn't do or say.

The phrase "deepfake" comes from the combination of the terms "deep learning" and "fake." While it doesn't have one universally agreed-upon definition, a deepfake generally means that a person in an existing video is replaced with someone else's likeness. Essentially, a deepfake is a photo, audio, or video that has been manipulated by Machine Learning (ML) and Artificial Intelligence (AI) to make it appear to be something that it is not.

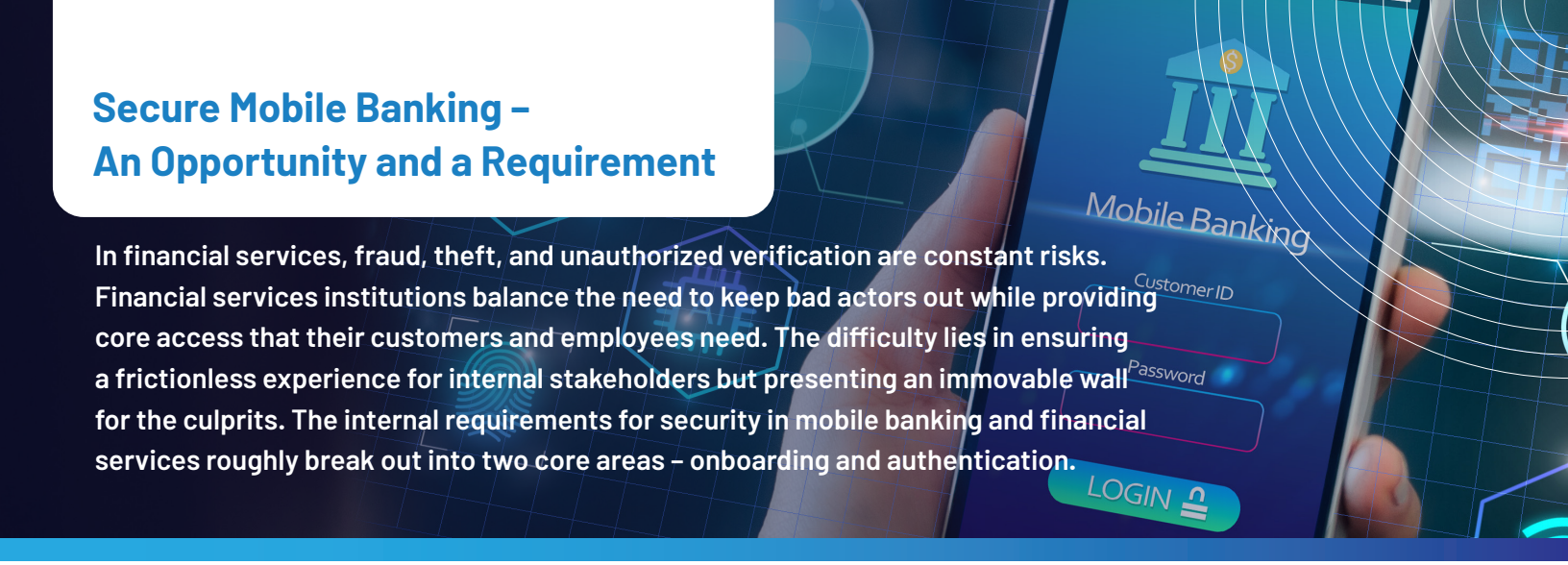
Deepfakes are not videos that have been reworked by video editing software. Specialized applications or algorithms usually generate them by blending old and newly manufactured videos. These deepfake applications, rooted in machine learning, deconstruct the subtle features of someone's face and learn how to manipulate them based on the individual conditions of the video. Those manipulations can then be integrated into a second video, making an entirely new creation.

The results are a synthetic video that could be used with good or bad intent. When considering a synthetic video, it's not hard to imagine why it might be dangerous. There's the obvious risk that a person's synthetic words or actions could incite someone to do something bad or dangerous. But an additional risk is that synthetic videos might start to undermine the believability of genuine videos. Privacy experts are understandably concerned that a deepfake might be used to spread misinformation on social media or bypass security measures intended to catch bad actors in the financial services industry from doing things like creating accounts or accessing funds.

Other Evolving Threats

The concerns don't stop at deepfakes. Morphs are a type of biometric attack method that combine the faces of two or more individuals into one unique face. Because there can be elements of an authorized user and an unauthorized user's face in the morph, less robust facial recognition technology could be tricked into providing fraudulent access. Morphs may also be used to fabricate identity documents, such as passports, for individuals who cannot lawfully get one, cross borders, or open financial accounts. In this instance, a morph would be created by combining the likenesses of the person who cannot get a passport with a person who can. This morphed image could then be used to enroll for a new passport. Once the passport is received, the unauthorized person could use it to "legitimately" do anything from bypassing border security to opening a bank account.

Secure Mobile Banking – An Opportunity and a Requirement



In financial services, fraud, theft, and unauthorized verification are constant risks. Financial services institutions balance the need to keep bad actors out while providing core access that their customers and employees need. The difficulty lies in ensuring a frictionless experience for internal stakeholders but presenting an immovable wall for the culprits. The internal requirements for security in mobile banking and financial services roughly break out into two core areas – onboarding and authentication.

Traditional Financial Onboarding and Authentication

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. Authentication, subsequently, constitutes any time a customer needs to access their account to move money or make a change. Historically, 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 shifted to more mobile solutions that could be performed online. Today, most financial institutions provide their customers with a means to complete transactions online or from a mobile device. But financial institutions have their work cut out to keep customers satisfied on this front.

A lengthy or complicated onboarding process deters potential customers. They expect a smooth, fast onboarding experience. And customers don't expect to have that experience in person; it needs to be digital.

The Challenges of Contemporary Onboarding

While in-person onboarding is certainly a tried-and-true method of customer registration, there are several challenges to current procedures for any remaining financial institutions that don't allow digital onboarding. 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 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. 32 percent of consumers refuse even to start an application if required to take ID credentials to a branch.[4]

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 percent 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 2021, it was found that 81 percent of hacking-related breaches used stolen and/or weak 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. The average person has 150 online accounts that require a password.[6] To remember them, people tend to base their passwords on information 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 percent 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 Security, Onboarding, and Authentication

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, with 63 percent of respondents in one survey saying they use their mobile banking app often.[9]

Despite consumers' positive reactions and 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 financial institutions face from contemporary mobile onboarding and authentication procedures.

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 during the authentication process:

Stopping 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 the 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. Facial recognition makes these types of attacks much more difficult, and adding voice biometrics, makes them even less likely to succeed. 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 the 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 also prevents this type of insider attack.

Mobile-Based Onboarding

Facial and speaker (voice) recognition are valuable tools for 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 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 "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 compared to the stored biometric, and access is granted.

One key advantage is that, unlike passwords, biometrics cannot be stolen or guessed. Biometrics use something 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 biometric measures in place, banks and financial companies can be sure that the customers being onboarded are not impostors 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 security and convenience within financial services. In contrast to remembering 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 frictionless 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. 66 percent of people have used biometrics and view them as easier and faster to use than traditional passwords.[10] One study revealed that 67 percent of adults from across the U.S., Asia Pacific (APAC), and Europe are comfortable using biometric authentication today, while 87 percent say they'll be comfortable with these technologies in the future.[11]

The Future of Mobile Banking Lies with Biometrics

Consumers' expectations of their mobile banking apps and financial services portals continue to rise, particularly as the world turns 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, banks and other institutions are increasingly viewing biometrics as a business imperative and a future reality.

Interested in learning more? Visit www.aware.com

Sources:

1 - www.bankmycell.com/blog/how-many-phones-are-in-the-world
2 - www.statista.com/statistics/1228757/online-banking-users-worldwide/
3 - javelinstrategy.com/webinar/2021-child-identity-fraud-study-key-findings
4 - www.signicat.com/battle-to-onboard
5 - www.verizon.com/business/resources/reports/dbir/
6 - blog.dashlane.com/world-password-day/
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.provident.bank/press-releases/provident-bank-study-shows-digital-banking-still-the-banking-method-of-choice-by-consumers
10 - https://usa.visa.com/visa-everywhere/blog/bdp/2020/01/02/banking-on-biometrics-1578003687083.html
11 - https://newsroom.ibm.com/2018-01-28-IBM-Future-of-Identity-Study-Millennials-Poised-to-Disrupt-Authentication-Landscape