Shufti Pro

Identity Verification

Banking on Biometrics

The Future of Customer Authentication in the Financial Sector

What's Inside

Passwords - Are they secure? 03

Biometrics as a Means of Authentication 04

What is biometric authentication? 04

Identity and biometrics 05

Adoption of Biometrics in Banking 06

History of biometrics usage and market cap 07

Most popular biometric modalities for the financial sector 09

Fingerprint scanning 09

Face verification 10

Voice recognition 10

Iris Scanning 12

Application of biometrics in banking 13

Biometrics in customer onboarding 13

Biometrics in ATMs 13

Biometrics in mobile banking 14

Using Biometrics for Better Customer Experience and Enhanced Security 15

Advanced customers want smart choices 16

Your Customers are On Board - Are you? 17

Enlisting third party experts with proven track 18

Seeking for cross-channel 18

“Biometrics represents a major change in how digital transactions are secured”

Raymond Liao, managing director at Samsung NEXT Ventures

The financial industry flourishes on security and safety. Yet that is precisely what passwords, PINs, and other knowledge-based authentication does not offer. They can easily be forgotten, stolen or hacked. Microsoft announced that a staggering amount of 44 million users are vulnerable to account take over attacks due to compromised passwords.[1] One of the basic weaknesses of the passwords is that people repeat or simplify passwords for their convenience which makes them easy to guess or hack. A survey by Google found that at least 65% of the people reuse passwords across multiple sites, making it vulnerable to identity theft and financial frauds.[2]

[1] Zdnet - 44 million microsoft users

[2] Google - Security infographic

Passwords - Are they secure?

Passwords with long phrases containing a combination of numbers, letters, and special characters have been a de facto security instruction for more than a decade. Even though experts recommend using strong, complex passwords for securing sensitive and personally identifiable information against criminals who can engineer numerous ways to snatch it from under your nose, does it stand up to scrutiny? According to research, the average person has 70-80 passwords.[3] Would it be possible to remember this many passwords? Even if a person is capable of remembering all their passwords still the question about the safety remains unsolved. Data breaches result in passwords being compromised and used for illicit financial and criminal activities. In the first six months of 2019, 4.1 billion personal records were exposed.[4] Instead of unsecure and difficult to remember passwords, the financial industry that heavily relies on security and safety is looking into other options that are both safe and convenient for the users.

There are several alternatives to the passwords currently being deployed but their security and convenience is still a question. For instance, token authentication is used as a security protocol by many organisations but they are not so convenient for the users. Similarly, two-factor authentication which is widely adopted has some drawbacks such as the user may not have access to the mobile phone when a security code is sent for authentication. So what technology is suitable to replace passwords? What steps world-leading banks, brokerage, investment and insurance firms are taking to provide swift and convenient access to the customers while enhancing security?

[3] NewsWire - New research

[4] Forbes - Data breaches expose

Biometrics as a Means of Authentication

The answer is biometric authentication. In this whitepaper, we will discuss how leading financial services firms across the globe are embracing biometric technology as a means of customer authentication and abandoning old traditional security methods to provide a secure and friendlier experience for their customers. But first, let us discuss the biometric options available to them.

What is biometric authentication?

Biometric authentication is simply recognizing and verifying a person's identity based on their unique physical and behavioural traits like the way a person walks, or unique patterns on their fingerprint or face.

Once an amazing theme of science fiction movies, biometrics today have become highly sophisticated, advanced and secure. Additionally, it is becoming increasingly commonplace. Today, a vast majority of consumers use biometrics to unlock their smartphones, sign in to apps and even conduct online transactions.

It is not only manufacturers that are embracing the technology, but the banks and other financial institutions are also adopting the biometrics at large scale.

Acuity estimates that by the end of 2020, 65% of all mCommerce transactions will be authenticated by biometrics.[5] Another estimate indicates that only in the financial sector biometric value could reach $8 billion by 2020.[6]

Identity and biometrics

There are three possible ways to prove someone's identity:

Something you have:

It is generally the easiest method for verifying identity. Most commonly an individual is authenticated using ID documents issued by any authority.

Something you know:

Most commonly used way for verifying identity is by using passwords, PINs, or any other knowledge that only a person could answer.

Something you are:

Considered as the most convenient and secure method, verification through your fingerprint, face and hand is known as something you are.

[5] Financialit - All content with rss

[6] NSTS - Biometrics for payments

Adoption of Biometrics in Banking

The swift digitization of banking services and the continued need to adopt stricter customer and employee identification protocols to prevent identity theft and frauds has set the table for biometric authentication technology to become an integral part of financial industry's security platforms. Additionally, the capability of biometrics to act as a strong authentication tool to help secure ATM, brick and mortar and online transactions, biometrics also help to increase customer trust and brand reputation. According to a survey by data vendors, 65% of the consumers agree to feel more comfortable in using some form of biometric to secure their payment details.[7] With the necessity for a stronger authentication solution becoming inevitable, because of the growing transactional technology adoption, an unfortunate rise in fraud and security breaches due to reliance on the traditional security systems is observed.

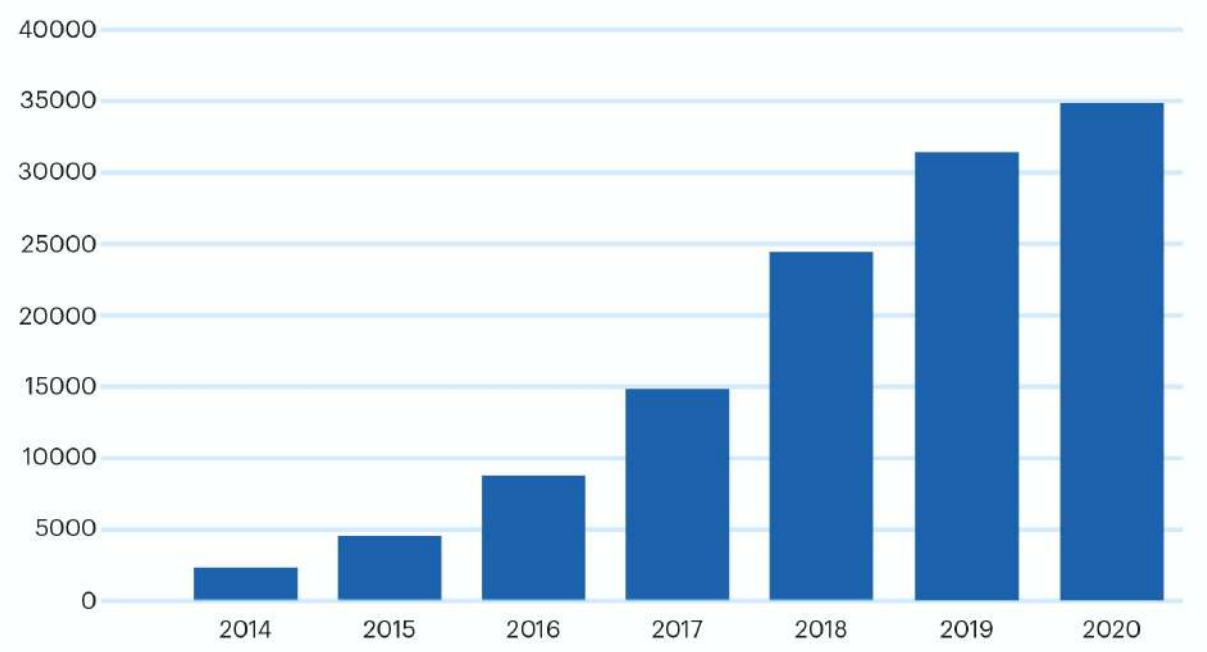
[7] Biometric update - Biometric and future of payment transactions

History of biometrics usage and market cap

Despite high scepticism on how the biometric market will develop in the next few years, expectations are positive. For example, marketsandmarkets estimates that the biometrics market will grow to $65.3 billion by 2024 with a CAGR of 14.6%.[8] Another estimate indicates that the global biometrics market will reach $22 billion by 2020.[9] These statistics include biometrically-enabled smart devices, biometric sensors, contactless biometrics, service kiosks, etc.

Biometrics Market Cap

Mobile biometric revenue (USD millions)



Source: Acuity

[8] MarketsandMarkets - Next gen biometric

[9] Global News Wire - Access control market

In the financial sector, biometrics is not unchartered territory. Banks have been exploring options such as fingerprint scanning for decades, it is actually the convenience and availability of smartphones which is making biometrics available to everyone.

A 2012 survey among 121 banks using biometrics at that time revealed that they prefer this technology.[10] Nonetheless, other biometric technologies falling under the umbrella of contactless authentication, such as the face, voice and iris recognition are gaining ground and can potentially provide greater versatility and convenience. In any case, biometrics is expected to replace the era of physical cards, logical PINs and passwords as security measures, providing the opportunity to develop a more integrated environment.

[10] Researchgate - List of 121 banks

Most popular biometric modalities for the financial sector

Here are the most popular modalities in the financial sector:

Fingerprint scanning

Initially, fingerprints were used by law enforcement agencies to identify and verify criminals. Today, a large population is using fingerprint sensors as a security measure in their smartphones. The global fingerprint sensing shipments are expected to reach 1.1 billion units in 2020 with a projected increase of 200 million units in three years.[11] In response, leading banking institutions like Bank of America now offer fingerprint sign-in to consumers on android and iOS banking applications.

Since customers are already used to unlocking their smartphones with fingerprints and making purchases online, it's natural that they will feel comfortable onboarding using fingerprint authentication in banking and other applications. Up till now, the most progress in this space is centred on mobile applications. However, fingerprint scanners are also becoming mainstream authentication at bank branches. For example, in 2014, Poland became the first country in Europe to introduce finger vein recognition on 2000 ATMs at bank branches and supermarkets.[12] Similarly, many Japanese banks use the same technology to monitor access to safety deposit boxes in branches.

[11] Statista - Global fingerprint shipments

[12] In the Loop - Forget fingerprints

Face verification

Face recognition is commonly used in security surveillance in high traffic public areas like border crossings, airports, train stations and stadiums but facial recognition software is making its way to the mainstream financial sector. The concept of 'selfie banking' is becoming increasingly popular. Around since 2016, selfie banking is a new way to onboard customers by allowing them to set up accounts by simply taking a selfie which is compared with the picture on the govt-issued ID documents.

The advantage is simply; the convenience as the customers will not have to visit a bank's branch for opening the bank account and with AI-enabled technology combined with live biometrics seamless security is offered. Additionally, face authentication is being gradually adopted for authenticating online transactions. Apple Pay, Selfie Pay and AliPay are examples of facial biometrics being used for transaction authentication. In terms of financial institutions, USAA became the first major bank to adopt facial biometrics for transaction authentication in 2015.[13]

Voice recognition

Voice recognition allows customers to use their own voices in place of hard to remember passwords and PINs. According to a 2019 survey conducted by the Harris Poll, 51% of the consumers in the US saw potential benefits to voice-activated banking up from 41% in 2017.[14] With major releases by HSBC, US Bank, Royal

[13] Bizjournals - USAA members

[14] Benori Knowledge - Evolution of voice banking

Bank of Canada, and CitiGroup, voice biometrics in banking is exploding. As per research by Juniper, 8 billion digital voice assistants are expected to be in use globally by 2023, up from 2.5 billion assistants in use at the end of 2018. The report also predicted that voice commerce will reach USD 80 billion by 2023.[15] Voice-activated banking was introduced in 2014 and since then it is gaining popularity. Here's a list of banks that adopted voice-activated banking:

Bank	Country	Launch Year	Key Features
Aisa Pacific			
KEB Hana Bank	Korea	2017	Account enquiries, track spending, financial news
Shinhan Bank	Korea	2017	Account enquiries, track spending, financial news
Woori Bank	Korea	2017	Account enquiries, track spending, financial news
OCBC Bank	Singapore	2017	Account enquiries
ICICI	India	2017	Account enquiries, financial news, credit card details
HDFC	India	2018	Account enquiries, payment dues
Ant Financial Service Group	China	2018	Account enquiries
ING Bank Australia	Australia	2018	Account enquiries
National Australia Bank	Australia	2018	Account enquiries
Westpac	Australia	2018	Account enquiries, financial news, payments
CIMB	Malaysia	2018	Account enquiries, track spending, payments
Middle East			
Emirates NBD	UAE	2019	Account enquiries, financial news
UK and US			
Monzo	UK	2016	Account enquiries, payments
Barclays Bank	UK	2017	Account enquiries, payments
Starling Bank	UK	2017	Account enquiries, payments
Paypal	US	2016	Account enquiries
Capital One	US	2016	Account enquiries, track spending, payments
American Express	US	2017	Account enquiries, payments
US Bank	US	2017	Account enquiries, track spending, payments
USAA	US	2017	Account enquiries, payments
Enrichment CU	US	2017	Account enquiries, payments, loan payments
Ally Bank	US	2017	Account enquiries, track spending, payments
Bank of America	US	2018	Account enquiries, track spending, payments

Source: The Asian Banker

[15] Juniper Research - Digital voice assistants

Unlike passwords, voice biometrics cannot be compromised. Voiceprints are stored as a string of hashes and characters which means it cannot be used in the same way even if compromised. Plus every time a hacker interacts with voice-enabled IVR, their voice will be recorded and that can be used to keep them away from the system.

Iris Scanning

Biometric iris scanning automatically identifies an individual based on unique features or characteristics possessed by the person. It is regarded as a reliable and accurate biometric identity verification and is considered most secured in terms of confidential information. While traditional verification systems using passwords, PINs or any other knowledge-based authentication could easily be hacked, iris scanning is considered more secure. Earlier widespread deployment of iris scanners was typically found at airports for security screening but today millions of individuals are enrolled in iris scanning for travel expedites including the password-free border crossing. In the financial sector, Bank of America, National Bank of Qatar and numerous others launched their pilot programs for iris scanning at ATMs.

Characteristics	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	high	high	low	medium	medium	high	high
Error Incidence	dryness, dirt, age	hand injury, age	glasses	lightning	lightning, age, glasses, hair	signature	colds
Accuracy	high	high	very high	very high	high	high	high
User Acceptance	medium	medium	medium	medium	medium	high	high
Long Term Stability	high	medium	high	high	medium	medium	medium

Source: Biometrics and Face Recognition Techniques

Application of biometrics in banking

Biometrics is gradually displacing traditional passwords and token-based access, signature-based branch service access and PIN-based access in mobile banking and ATMs. Here are some ways that banks can use biometrics to improve customer services and secure customer assets.

Biometrics in customer onboarding

Financial services institutions can adopt biometrics for onboarding customers. Normally, the banks need end-users to undergo know your customer (KYC) verification as a part of customer due diligence. This usually requires a customer to visit the bank branch with their ID documents and the process may take several minutes and sometimes days. With customers becoming technologically advanced they are keen to get banking services, not the banks. Moreover, with the availability of systems like Netflix and Uber where customers could swiftly onboard, consumers look for convenience. By using biometrics such as face verification, banks could easily digitalise their onboarding process and provide convenient services to their customers with high security.

Biometrics in ATMs

Biometrics in banking ATMs are already popular in developed countries and adoption is significantly increasing. In ATMs, two

approaches are used for customer authentication - a customer using only biometrics and a PIN along with biometric authentication. Therefore, facial recognition and fingerprints are most suitable in ATMs as these biometric traits can easily be authenticated in this environment. Moreover, these biometric technologies offer advantages such as flexibility, compactness, and accuracy.

Biometrics in mobile banking

Mobile banking is growing rapidly and according to DataProt, 79% of the smartphone owners have used their device for online purchase in the past 12 months.[16] Another research highlights that 6.93% of the millennials used mobile banking in 2019.[17] Notwithstanding this large number, many bank customers still have a lack of trust over the security of mobile banking platforms as mobile app related fraud transactions have increased by 600% since 2015.[18] Online banking transactions or customer services could be performed through facial recognition as authentication using smartphone cameras.

Additionally, banks are required to monitor transactions and identify any suspicious transactions occurring over online banking. Facial biometric authentication could be used for ongoing KYC monitoring. With emerging cases of mobile banking fraud, banks need to ensure ultimate protection of customer data with sophisticated technologies. Biometric authentication can become an effective security measure for banking.

[16] Outer Box Design - Mobile e-commerce stats
[17] Dataprot - Mobile banking stats
[18] Finjan Mobile - Fraudulent transactions

Using Biometrics for Better Customer Experience and Enhanced Security

In each of the use cases, biometric technology represents a significant improvement in customer experience over knowledge-based authentication and provides valuable gains in efficiency and security. Biometrics offer significantly quicker, frictionless and secure authentication that passwords and PINs cannot. Firstly, biometric data is not stored in any identifiable way on either user's mobile devices or banks databases. Even if the hacker gets access to the device or penetrates the database, the information is almost impossible to retrieve or reassemble in a usable manner.

Moreover, it is extremely hard to fake biometric data. Although there have been some advanced technologies such as presentation attacks, deep fakes and 3D spoofing attacks that pose threats to the integrity of biometric authentication, with the advancement in biometric technologies, these attacks could easily be detected and dealt with. The latest biometric authentication systems use artificial intelligence and machine learning algorithms to counter such attacks. The most sophisticated technologies in use today include liveness detection, presentation attack detection, 3D depth-sensing, etc. that can determine the difference between an actual person and pre-record or synthesized voice/video/image or an actual fingerprint versus scanned rendition or modelled impression.

Advanced customers want smart choices

There is no doubt that consumers have higher expectations now than they did a decade ago. This is mainly because advances in technology and savvy business models now make it possible to turn historically poor experiences (like summoning a cab) into seamless, convenient and even satisfying ones (like booking a ride through Uber). For the financial industry customer verification and authentication has been that poor experience historically. The financial industry is bound to perform customer verification to fulfil the regulatory KYC and AML requirements and authentication to safeguard financial assets. According to a survey conducted by GlobalData, 67% of the global consumer would feel happy to use some form of biometrics to secure their data.[19] To comply with regulatory requirements, securing assets and at the same time provide seamless customer experience, banks need to provide smarter choices that fully empower customers to have a more effortless experience in nearly every circumstance.

[19] Global Data - Biometric replace passwords

Your Customers are On Board - Are you?

With the advancement in technology and customer expectations, many customers are in line to have better banking experience. GlobalData highlights that the adoption rate of biometric authentication is as high as 93% in banking customers if rolled out properly. Today it is not about if the banks and leading financial institutions will put efforts to replace knowledge-based authentication with biometrics or not. It is more about when will many recognize the security risks and poor customer experience inherent to knowledge-based authentication. More banks are adopting biometrics every day and more will follow the suit.

However, the question is which institutions will be able to deploy the technology effectively at scale with high returns ultimately associating their brand with high value, low-effort services that today's customers expect.

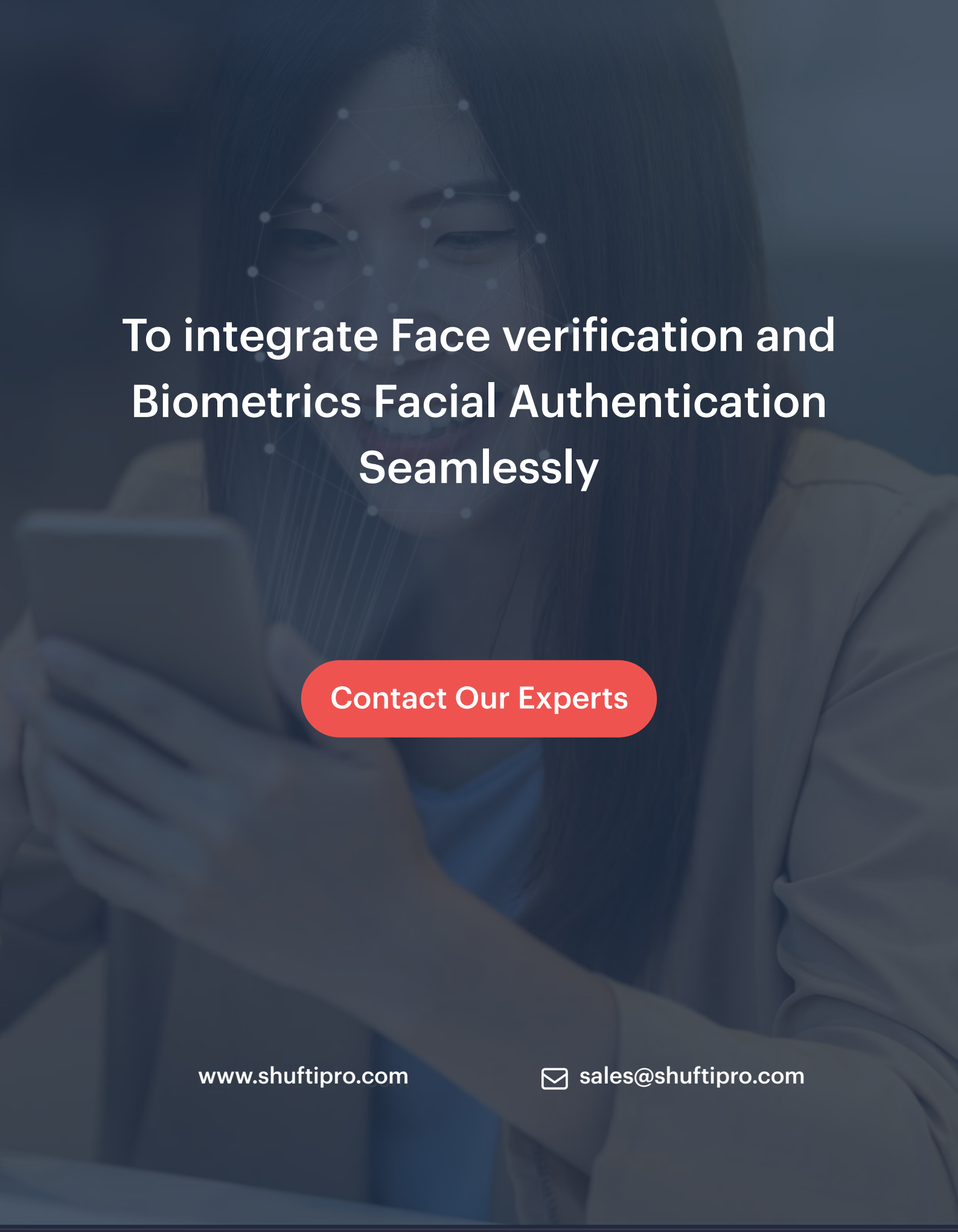
To get ahead of the curve we recommend:

Enlisting third party experts with proven track records

Since it is very difficult and expensive to build in-house verification and authentication systems, you'll want to partner with an organisation that has experience in developing and deploying seamless biometric technology.

Seeking for cross-channel

Even if your customer base is a mobile phone user, it is highly likely that they would be looking for the same features on the web application so it is recommended to seek for applications that provide authentication and verification features in both mobile and web applications.



To integrate Face verification and Biometrics Facial Authentication Seamlessly

Contact Our Experts

www.shuftipro.com

sales@shuftipro.com

Shufti Pro

Shufti Pro

True Identity Builds Trust

Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from 3000+ ID templates and business entities from 200 million companies data.