Shufti Pro

Fintech Customer Onboarding Through Video KYC

White Paper

Table of Contents

Fintech Industry - An Overview

Fintech or financial technology is a term that refers to the use of technology to improve financial services and make them more efficient. It is a rapidly growing industry serving both consumers and businesses. From mobile banking and insurance to cryptocurrency and investment apps, fintech offers broad applications to all of them. As a driver of the digital economy, Fintech has the potential to revolutionize financial sectors through innovative financial solutions.

Since its inception, the fintech industry has caused the biggest disruption within the financial services industry. In 2016, this sector witnessed a huge boom as it developed new banking technologies that perpetuated an industry-wide change.

The fintech industry managed to gather an investment of US $9.4 billion in the second quarter of 2016 [1], wherein China, the fintech sector revenue increased by 55.2% from 2016 to 2017 [2] and is estimated to reach 1.97 trillion yuan by the end of 2020 [3].

>> Whereas globally, the Fintech market is expected to grow at an annual growth rate (**CAGR**) of **6%**, making it worth **$26.5** trillion by the year **2022** [4].

Using technology and software, fintech powers mobile payments, insurance, crowdfunding platforms, investment, as well as cryptocurrency and blockchain. In simple words, it's an emerging industry that aims to streamline financial flows and manage finances to improve user experience and service delivery in the market.

Fintech organizations around the world are valued in billions of dollars, with companies such as Adyen, Qudian, Avant, and Ant Financial present at the top of the list [5]. In 2019, Fintech investments reached $55.3 billion, with close to half the amount coming from China [6]. For the common man, services like Square, Swipe, Venmo, WePay have altered the way they perceive lending and payment transactions. Further, in the second quarter of 2019, the mobile cash app, PayPal, recorded a 17% year-on-year growth and registered 286 million accounts active globally [7].

With consumer-focused applications, technology has moved from the back-end of banking platforms directly into the hands of the end-user. We can now easily manage and track funds, and investments with just a tap away, as most of the services, are now accessible from smartphones and tablets. With the technology-focused consumer behavior, the fintech industry is set to unlock further milestones in the future

According to Adroit market research, the global fintech market size is projected to reach US $460 billion by 2025, and its global market value to reach $305 billion in the next five years [8].

Need for Identity Verification

Identity verification is important to protect companies and their customers from criminal activity. A person's identity is integral to procuring goods and services and the fraudulent use of this personal information can be harmful to both entities. **Given the rise in fraudulent activities, a report from PwC reveals that approximately 28% of the banking and payment businesses are at risk in 2020[9].**

Furthermore, the 2020 Identity Fraud Report by Javelin Strategy & Research revealed that identity frauds in financial institutions grew 15% in 2019 to $16.9 billion [10]. These fraud cases and revenue loss stats reveal that user identity is one of the major targets of criminals in the financial industry and therefore the financial organizations must perform robust digital identity verification of remote customers they are onboarding and the individuals with whom they are doing business with.

By verifying the identity of customers, fintech institutions and businesses can manage risk more effectively. A customer's history gives such organizations risk indicators and helps to determine how likely these individuals are going to harm their organization.

Identity verification procedures protect businesses against:

- ✅ Facilitating money laundering
- ✅ Trade of illegal goods
- ✅ Terrorist funding
- ✅ Political corruption
- ✅ Market manipulation
- ✅ Penalties from regulators

KYC and AML regulations

The Fintech market is growing at an extraordinary pace around the world, and this makes it difficult for financial regulators to understand these new technologies and how they fit into the existing regulatory framework. Regulators are aware of the need for innovation in this sector, so they try to support and promote fintech activities through actions such as the creation of regulatory virtual spaces. For instance, the UK's Financial Conduct Authority (FCA) that is in-charge of regulations in fintech industry has initiated 'project innovate' and 'regulatory sandbox,' in the UK to help companies introduce and test new financial projects and distribution methods, establishing the UK as a leader in fintech and a global authority on fintech regulation [11]. FCA also encourages businesses to perform AML and KYC checks to secure their firms from unwanted risks.

These regulators on the other hand, also don't want the existing risks including cybercrimes, money laundering, and online identity theft, etc, to increase with the growth of the fintech industry. For that, on May 24, 2019, Financial Crimes Enforcement Network (FinCEN), a

regulatory authority in USA announced that it would begin holding monthly "Innovation Hours" designed to offer financial institutions as well as fintech and regtech organizations the opportunity to present their innovative products, services, and approaches designed to enhance AML efforts [12].

Therefore, the fintech industry has to comply with the KYC and AML regulations just like banks to keep the financial environment safe for users.

KYC (Know your customer)

KYC can be described as the practice carried out by companies to verify the identity of their customers.

In fintech, KYC procedures are applied to existing and new customers to identify and prevent risks. KYC plays an important part in eliminating the risks associated with money laundering, terrorist financing, fraud, corruption, bribery, and other illegal financial activities. Fintech businesses must perform robust KYC procedures to detect and prevent crime risks associated with the development of technology.

AML (Anti Money Laundering)

Anti-money laundering (AML) refers to a set of laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income.

Fintech platforms are a potential target for money laundering criminal organizations around the world because of the increase in the rate of initiation of transactions in these systems, and the unlimited money flow. With the increase in the circulation of digital money, criminals continue their money laundering activities in this direction.

To avoid the risk of money laundering, fintech platforms must comply with AML regulations specific to the regions they work in and must develop an effective compliance program to prevent the risk of financial crime.

What Is Identity Verification?

Identity verification is a process that ensures a person is who he claims to be. Identity is a set of unique traits and characteristics associated with a unique human being. These traits become essential when businesses have to deal with people within the online environment, where identity theft is a more common phenomenon than we think [13].

Identity verification has become an essential requirement in most processes and procedures, both online and offline, from opening a bank account to completing tax procedures electronically. This process is mostly carried out by banks, and other businesses by which they verify that a customer is exactly who they claim to be so they can receive certain services that are subject to regulations. The identity verification process in industries like fintech or banking is more commonly known as the KYC process.

There are three main factors of identity verification.

- Collection and verification of identity proof (identity documents such as ID card, Passport, etc.)

- Verify biometrics details (e.g. face, fingerprint or voice)

- Background screening (AML screening)

Document and Identity Frauds

With the development of technology and increasing competition, consumers demand quick onboarding services from businesses, leaving very little time for them to perform verifications effectively. **HubSpot reveals that 33% of the customers are most frustrated for repeating the customer support steps [14].** This increases the chances of document and identity fraud in the fintech industry. Let's discuss a few of the most common types of ID fraud that businesses face.

Forged documents

There are various types of forgeries in the documents, but they all start the same. Fraudsters change information on the document to modify the identity of a person. It can be a complete change or a partial identity modification.

The change may include:

- Change in variable information

- Inserting real pages from another document

- Removing pages or specific information

- Applying false stamps or watermarks

Counterfeit documents

Similar to counterfeit money, counterfeit documents are imitations or reproductions of the original ones. A fraudster typically obtains a template and inserts fake details and images in it. These templates are illegally purchased and highly advanced counterfeits are easily available on the black market.

Fraudulently obtained documents

To obtain such documents fraudsters lie on their applications in a myriad of ways, they may use a stolen photo applied on a fake document or use different personal details for authorities to issue them original, authentic documents that contain false information.

Blank stolen documents

Every authentic document starts out blank, but they become fraudulent when fraudsters leak these blank or un-personalized original documents from the manufacturing supply chain and fill in fake information for scam purposes.

Other types of online frauds associated with the fintech industry include:

Synthetic identity fraud

This is a type of fraud where scammers create new identities by combining fake information with stolen original data. Scammers steal information from users like addresses, IDs, phone numbers, etc. through social media platforms and incorporate it with fake data. This way they create fake but believable data which is often undetected and very dangerous to business organizations. **According to a Federal Reserve study, synthetic identity fraud is the fastest-growing financial crime in the US, with an average charge-off balance per instance of $15,000 [15].**

Account frauds

Account frauds are another type of unique fraud in the fintech world where scammers disappear after stealing large amounts of money from banks. These types of scammers usually have a good credit score maintained for a long time, created with the help of fabricated or

unrealistic information related to incomes from stolen identities and then at once they withdraw large amounts of loans and disappear which then leads to bad debts in the lending company and eventually losses. Other popular types of account frauds include:

New account fraud

New account fraud, also known as account opening fraud occurs when a fraudster uses stolen or synthetic identities to open new bank accounts, maxing out their credit limits before disappearing into thin air undetected. **According to RSA Security, 48% of all fraud value stems from accounts that are less than a day old [16].**

Account takeover fraud

In account takeover fraud the perpetrator illegitimately gains access to a person's online financial accounts commonly through the use of bots. This results in multiple fraudulent transactions and unauthorized orders carried out from the breached accounts. **According to Tech Republic, account takeover frauds increased by 282% due to the coronavirus lockdown [17] .**

Payment frauds

These frauds happen when scammers make large purchases under stolen credit cards or identities. The quick transaction processes these days usually give very little time for the businesses to verify the authenticity of the user. The fraud is detected when the victim reports the loss of money in their account, and the company ends up paying compensation to the victim.

Methods of Identity Verification

There are various methods that fintech platforms employ for the verification of their customers or clients. Let's discuss a few of the most common methods.

Private or official databases

Databases are the are systems that house data, that is previously collected and verified as part of a registration system. They can be private databases run by profit organizations or public databases run by governments. For example, private databases include credit bureaus and telephone directories and public databases include government identifiers (Social Security, tax or voter numbers) or the DMV (Department of motor vehicles) that houses driver's license data and numbers. While using databases for identity verification, there are certain things that must be considered first including the cost of access, the fact that previous data breaches (if any) may have compromised the credibility of the data, and whether it can be used commercially under current privacy regulations .

Online verification from ID documents

In online verification, various techniques including artificial intelligence, human intelligence, and facial recognition, are used to determine if a government-issued id document belongs to the user trying to enroll in the system. This method typically requires users to

provide a picture of themselves holding an ID document, thus ensuring the person on the ID is the same person holding that document.

Government-issued ID documents might include:

- National identity card
- Driver's license
- Passport
- Residence permit
- Voter identification document
- Tax identification document

Two-factor authentication (2FA)

This method requires users to provide a form of personal identification, also known as a token, in addition to the usual username and password details before they can access an account. The token is like a code that can be a number or an alphabet that the user receives from the authenticating agency during the sign-up or login process. 2FA is particularly useful for creating accounts and resetting passwords,

however, this method typically requires users to have their cellphones with them during the authentication process.

Shufti Pro's allows businesses to integrate an extra layer of security for customer onboarding and verification through its two-factor authentication feature. Shufti Pro 2FA allows:

Quick and smooth customer onboarding within 5 seconds

Identity fraud prevention and financial loss mitigation for end-user accounts

Decreased reliance on traditional single-layer security methods

Authorized customer account access to keep sensitive information safe

Knowledge-Based Authentication (KBA)

KBA verifies a person's identity by requiring an answer to security questions. These questions are generally designed to be easy for the user's to easily remember them. For additional safety, this method allows you to place a requirement for users to answer the questions within a specified time limit. KBA being the easiest verification method for users to understand has a drawback, as it is getting increasingly

easy for hackers to discover the answers via social networking sites and other more traditional forms of social engineering.
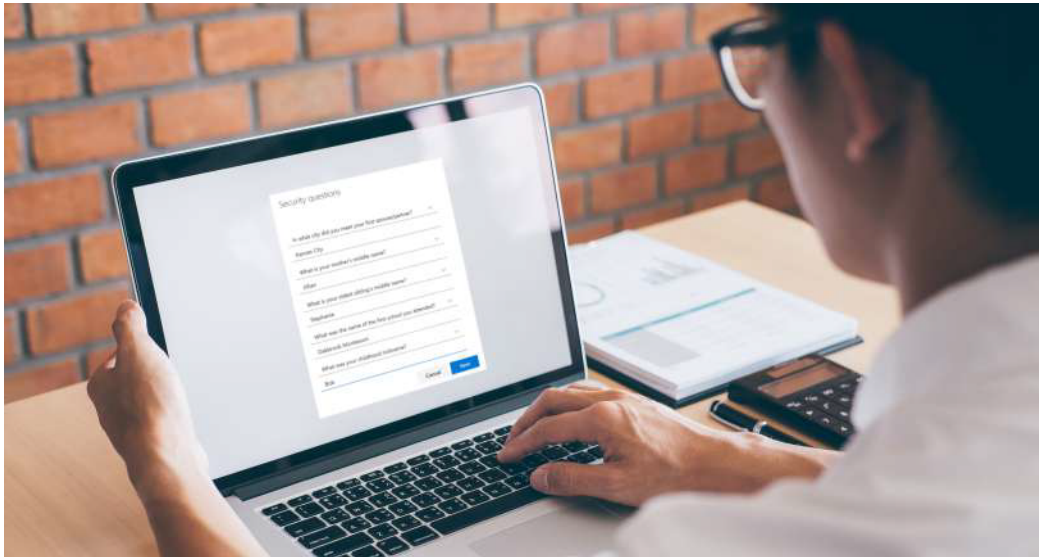
Visual document authenticity

You can check the authenticity of an ID document through its images being provided by the user. It helps to spot the forgeries that might be more prevalent when a human inspector is not present. There are several ways to evaluate the ID and user, which can help identify possible tampering and impersonation from multiple perspectives:

Document template comparison: Comparing the submitted ID image against the known document template can identify errors or fake formats.

Font anomalies: Scammers often try to change fields of data but will leave behind font inconsistencies while doing so.

Security features: All ID documents have some form of built-in security features which while evaluating can ensure authenticity or reveal errors.

Facial comparison

In addition to confirming the authenticity of the ID document, we need to confirm that the user presenting the ID is its original or authorized owner. This can be done by asking the user to take a live picture while holding their identity document in their hands. By comparing the facial traits of the live picture with the photo in the ID card we can confirm the facial similarity and the authenticity of the user.

How to Detect Identity Frauds

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or perform other illegal activities. Therefore the sooner identity fraud is detected, the lower the financial impact. Follow these steps to recognize or detect the warning signs of identity fraud.

Data integrity analytics

Many ID documents have built-in security features that can be systematically checked to ensure the document is authentic or not. Such features can be described as:

Data validations: An ID document must contain valid data in specific defined places. Such data includes encoded MRZ areas that use check digits to protect data integrity. For example, gender, document registration numbers, expiry date and date of birth, etc.

Algorithm validations: Some documents include very specific embedded rules, in the form of mathematical algorithms, to identify any flaws in ID integrity.

Data consistency: There are certain data fields in multiple locations on an ID document that must match to prove its authenticity, like machine-readable formats, which when decoded will map directly to fields presented in clear text. Such data includes the date of expiry, document type, nationality, issuing country, document numbers, gender, date of birth, first or last name.

NFC chips: On many IDs, there is an NFC chip present containing additional information about an individual. Appropriate readers can access that information and compare it to information displayed on the ID.

Customer Identity Verification in Fintech Industry and The Advent of Video Interview KYC

Remote verification of customers can be done through various methods that are described above, but those methods can sometimes prove to be time taking or result in unwanted errors. However, another method of customer verification is becoming more and more popular in the identity verification market. This method is called Video KYC, and it is now grooving in the digital space for remote verification of customers.

What is Video KYC?

Video KYC is a video identification process that identifies and verifies a digital identity through a live video call and document verification. It helps reduce online fraud and ensures the onboarding of a credible customer.

It is a convenient and quick method in which a KYC expert onboards a customer and performs real-time identity verification. Video KYC is a secure method, helping Fintech businesses in attaining a clean customer base. It also makes KYC/AML compliance easy when it comes to verifying the customers in a digital world.

In the video KYC process, live KYC is performed and the customer or end-user is guided in real-time to show the identity document to the camera for document verification. The KYC expert asks a few questions from the end-user just like in-person KYC screening while observing their behavior.

Process of a live video interview

The video KYC process undergoes the following steps:

- The customer is asked to fill in the registration form that is present on a company's website.

- After the registration process, the KYC expert connects with the customer for live identity verification.

- The customer is guided for the process of identification through a video and liveness detection is performed to ensure the physical presence of a customer at the time of verification.

- KYC expert takes consent from the customer to collect data for identification purposes and to proceed forward.

- The customer is then asked to show (both sides) of ID document that could be an ID card, passport, or a driving license.

- The AI-based identity verification solution verifies the ID document, performs facial recognition, and AML screening.

Why video KYC is good for Fintech businesses (Benefits)

Video KYC ensures regulatory compliance for Fintech businesses by keeping a balance between digital security and customer experience. The following are some benefits of video KYC for fintech platforms:

Saves time and money

Video identification is a quick and cost-effective solution that fintech companies can use to perform digital identity verification of their customers.

Improves Digital Security

Video KYC reduces the risks of fraud and bad actors that use fake identity credentials and documents to get an entry into the digital financial system. This identification method checks the human body language and verifies the information in real-time to prevent digital scams.

Complying with KYC requirements

With live video identification, fintech platforms can meet the requirements of regulatory bodies to prevent financial crimes.

Enhanced customer experience

With Video KYC the customers can verify their identity by showing up identity documents to the camera and answering a few questions asked by the KYC expert. The information provided by the users can be verified instantly with document identification and facial recognition.

# How Shufti Pro Helps?

Shufti Pro's robust video KYC

© Powered by ShuftiPro

Shufti Pro's video KYC enables swift and secure customer onboarding for fintech businesses by performing a live identification process that is faster and guarantees high security. The video KYC feature of Shufti Pro offers:

- ✓ KYC expert's live assistance for your customers

- ✓ Eliminate identity fraud with online verification

- ✓ Fast onboarding with human verification specialist

- ✓ Instrumental in resolving KYC/AML compliance issues

- ✓ Fully customizable features based on your industry

AI-powered facial recognition

Shufti Pro's facial recognition technology utilizes AI and HI to perform customer verification in just 5 seconds. During a live video interview with the customer, the AI-powered facial recognition technology captures the customer's face picture and identifies various fraud with the help of the following checks:

Show your full face in camera
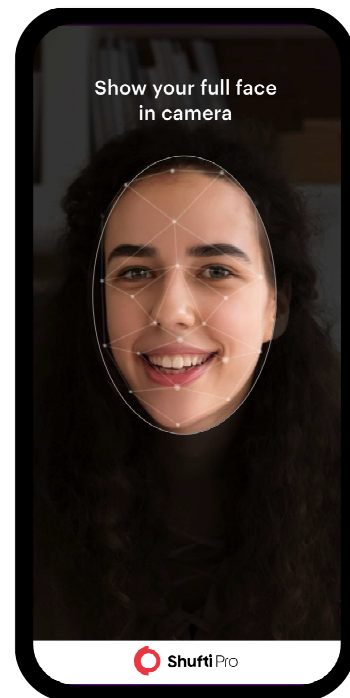
Shufti Pro

- Liveness detection
- Microexpressions analysis
- 3D depth perception
- AI mapping techniques
- Anti spoofing checks
- Fake image detection
- Human face attributes analysis

KYC and AML compliance solution

Shufti Pro provides top of the line KYC compliance and AML screening solutions that help businesses like fintech platforms to deter online frauds, digital scams, and for payment protection. While performing live customer interviews, thorough background checks are performed to screen out individuals that pose a financial risk for fintech businesses. Shufti Pro utilizes various verification methods to make sure that you only onboard legitimate customers and stay compliant with regulations. Those methods include:

- Face verification
- Document verification
- Address verification
- 2FA authentication
- Automated AML compliance

Shufti Pro's video KYC process

End-user registers on your platform

Live video call with KYC expert

End-user shows the identity document

Verification results are delivered

Three video KYC plans to fit your business

Shufti Pro offers three video KYC plans that businesses can choose according to their needs. Businesses can onboard customers with video chat through:

Regional KYC experts

Give a customized experience to your customers through regional KYC experts.

- Choose the nationality of your KYC expert
- Choose the language for verification process
- AI-powered screening of documents in real-time
- Instrumental in resolving KYC/AML compliance issues
- Don't have to hire ID verification experts

Use your own KYC experts

In this KYC plan businesses can:

- Choose their own KYC expert for verification

- Get identity documents screened in real-time

- Develop their customized identity screening plan

- Revamp their CDD practices

Automated AI-Based assistance

With this plan, businesses can achieve complete automation with Shufti Pro's AI-based solution, which gives:

- Automated AI-based identity verification solution

- AI-supported chat with the end-user in real-time

- Real-time OCR screening of identity documents

- No need to hire experts

Conclusion

With the rapid growth of the fintech industry, the fraud risks in this sector are increasing as well. This requires these financial organizations to adopt security measures that offer enhanced security with little to no chances of errors. Video KYC solution is the growing need of the hour to keep businesses protected and compliant with the required regulations. Shufti Pro's video KYC solution can help fintech businesses to onboard legitimate customers and stay ahead of their compliance needs.

Want to integrate Shufti Pro Video KYC in your system?

Contact our Expert

Apply for a no-commitment free trial

Get non-discriminatory access to all features of the

selective service of Shufti Pro for 15 days.

Get Free Trial

www.shuftipro.com   sales@shuftipro.com

Shufti Pro

References

1 https://www.ft.com/content/ce8fa350-737f-11e6-bf48-b372cdb1043a

2 http://www.iresearchchina.com/content/details7_41802.html#:~:text=Since%202016%2C%20the%
   20rising%20of,demographic%20dividend%20of%20internet%20industry.&text=In%202017%2C%20
   the%20revenue%20of,soaring%2055.2%25%20compared%20with%202016.

3 http://www.chinabankingnews.com/2018/10/29/fintech-china-expected-see-1-97tn-yuan-annual-
   revenue-2020-reshape-micro-enterprise-finance/

4 https://tipalti.com/fintech-stats-for-2020/

5 https://dev.to/seattledataguy/5-fintech-companies-disrupting-banking-and-finance-31nj

6 https://financesonline.com/fintech-statistics/

7 https://www.statista.com/statistics/218493/paypals-total-active-registered-accounts-from-2010/

8 https://www.globenewswire.com/news-release/2020/01/29/1976561/0/en/Fintech-Financial-
   Technology-Market-to-hit-460-billion-by-2025-Global-Insights-on-Growth-Drivers-Key-Trends-Strategic-
   Initiatives-Value-Chain-Analysis-and-Future-Outlook-Adroit-Mar.html

9 https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdfhttps:
   //www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf

10 https://www.javelinstrategy.com/press-release/identity-fraud-losses-increase-15-percent-consumer-
   out-pocket-costs-more-doubl

11 https://www.cfcunderwriting.com/resources/articles/2020/01/what-the-uk-can-tell-us-about-
   fintech-regulation/

12 https://www.globallegalinsights.com/practice-areas/fintech-laws-and-regulations/usa

13 https://cdn2.hubspot.net/hubfs/2109161/Final%20-%20Onfido%20Tech%20White%20Paper%20Oct
   %2018.pdf

14 https://blog.hubspot.com/service/customer-service-stats

15 https://www.finextra.com/blogposting/18267/top-10-cybercrime-and-online-fraud-predictions-
for-2020

16 https://www.technologymagazine.com/cloud-and-cybersecurity/dean-nicolls-addressing-problem-
new-account-fraud

17 https://www.techrepublic.com/article/account-takeover-fraud-rates-skyrocketed-282-over-last-year
/#:~:text=Account%20takeover%20(ATO)%20fraud%20attempts,and%20safety%20provider%20Sift%20
finds.&text=The%20index%20includes%20analysis%20from,US%20consumers%2C%20the%20
company%20said

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.