# KYC (Know Your Customer) in Fintech Industry

**Goutham Sabbani**

Business analyst, Media Systems Integration, UK

**Abstract:** ***KYC is a crucial regulatory and compliance element in the creation of fintech products, serving as a gauge for the prevention of fraud and financial crimes. Typically, it entails confirming and authenticating the identity of the customer, learning about the activities they engage in and where their funds originate, and evaluating the possibility of money laundering and terrorist funding. [1] Customer identification and verification are essential components of the customer due diligence process in digital financial services. [3] While it is evident that fintech companies, akin to other financial establishments, are obligated to conform to KYC and AML rules, it is equally critical to acknowledge that accomplishing so poses certain obstacles. [2] Here, we examine some of the major obstacles that the digital banking sector faces while completing KYC, which if resolved might greatly expand the sector's potential.***

**Keywords:** customer due diligence, anti - money laundering, enhanced due diligence, identity fraud, biometrics

## 1. Introduction

In addition to being known by a few other names, including identity verification, customer due diligence (also known as CDD), and know your client, KYC, or "know your customer, " is the phrase used to describe a collection of guidelines and procedures that are a part of anti - money laundering (AML) statutes including the Bank Secrecy Act. [2]

One of the biggest obstacles to financial inclusion is a lack of legal identification. Digital identity management solutions have the potential to facilitate greater financial inclusion by simplifying the administration and accessibility of identification. Novel approaches to e - KYC are being made possible by distributed ledgers, biometric data, artificial intelligence, and other technologies. [3]

According to Know Your Customer requirements, financial institutions must, in essence, know their customers by identity verification and have a comprehensive understanding of who they are. This enables federal agencies like FinCEN to "follow the money" after a crime has been committed and makes it simpler to identify cases of suspected money laundering, financing of terrorism, and other financial crimes. [2]

## 2. History of KYC

The U. S. Bank Secrecy Act (BSA), which mandated that financial institutions have procedures in place to identify and report suspicious behaviour, is where KYC first emerged in 1970. Due to this, anti - money laundering (AML) laws were enacted, requiring financial institutions to confirm the legitimacy of their clients. [4]

Governments realised they needed more laws in the 1970s and 80s due to an increase in high - profile instances involving organised crime, drug trafficking, and money laundering. As a result, the Bank of England introduced the first appropriate KYC standards in the early 1990s. [4]

The main goal of the Financial Action Task Force (FATF), an intergovernmental organisation, is to prevent financial crimes such as money laundering and financing of terrorism by creating international standards and best practices. The FATF went on to create a set of guidelines that would eventually be accepted as the best practice globally for preventing money laundering. Three main components comprised the extensive instructions on KYC procedures given in three primary components: - Customer Identification, Customer Due Diligence, Ongoing Customer Monitoring. [4]

**Requirements and Security**

Fintech and banks both have identical KYC standards. The client's name, address, phone number, and birthdate must be given. Fintech businesses must also use a government - issued ID card or passport to confirm the customer's identification. [3]It is also possible to choose to extract signals straight from the user's device, including their IP address, location information, device fingerprint, etc., and compare it with the data they give the customer directly. [2]

## 3. Challenges

**Cost**

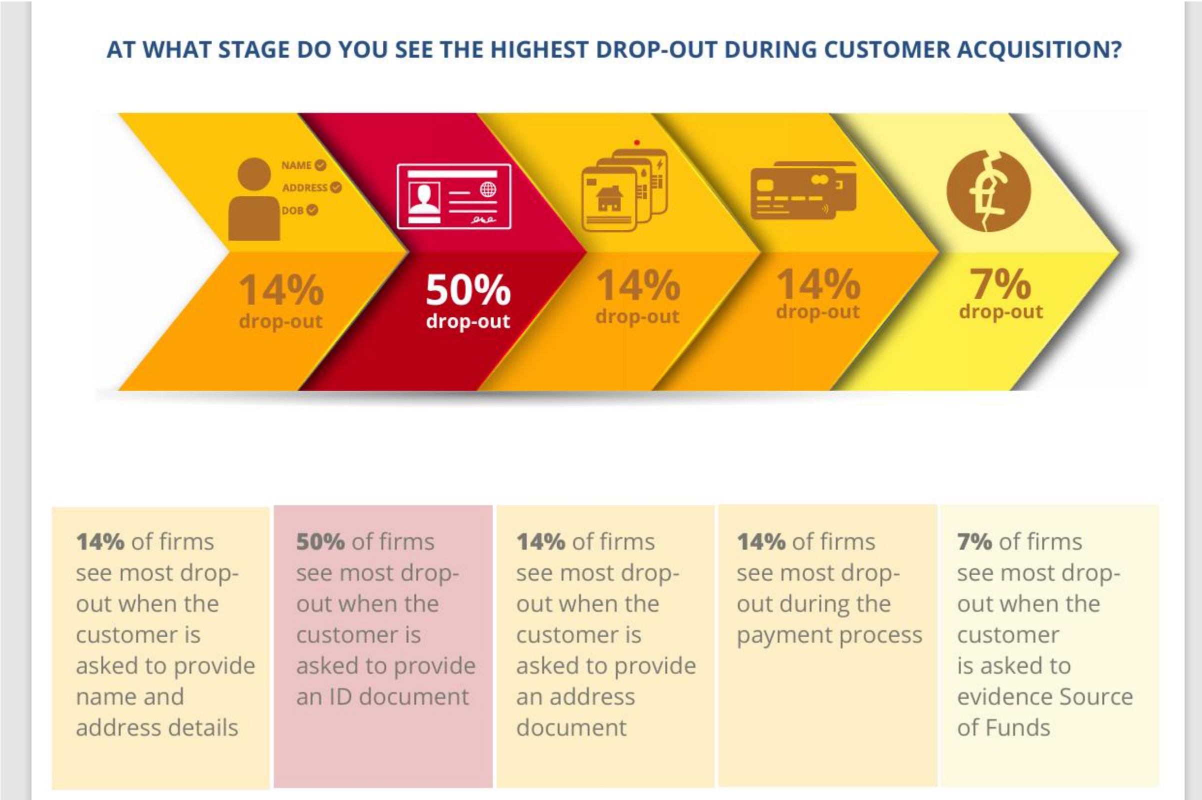
Even though traditional banking still handles a lot of these tasks manually, the rise of fintech has caused KYC procedures to become more digital. Fintech organisations are still facing several challenges, even though this change has greatly benefited both consumers and fintech providers, including faster and more effective onboarding and improved user experience. [1]

Hiring staff members in - house for these responsibilities is expensive in terms of time, money, resources, and compliance. As the fintech expands and scales, these costs will rise in tandem with demand and complexity, even if the brand is able to effectively absorb those costs through current operational or back - office operations. [1] Fintech companies can often waste money and time managing a disproportionate amount of false positive alerts, which is when their systems flag genuine customers for enhanced due diligence. [1]

**Losing customers**

To ensure compliance with the 2019 Money Laundering Regulations, companies must verify that the customer has supplied their true name, address, and birthdate. Database checks are one of the primary instruments used for KYC. Before a customer is onboarded, database checks are typically carried out programmatically in real - time, taking less than a second to complete and verifying their identification. The limits of this type of KYC are widely known in terms of match rate and geographic coverage, and not all consumers pass database checks. [5] When the database check is unsuccessful, the KYC and customer onboarding processes may take longer. Nonetheless, the average time spent by all companies is up to thirty minutes, suggesting that additional verifications after the first step are difficult and could jeopardise the customer's retention at the point of sign - up. Sadly, more than one - third of businesses take more than a day to finish the onboarding process. [5]

Figure below shows the stage and reasons why fintech customers dropped out during acquisition

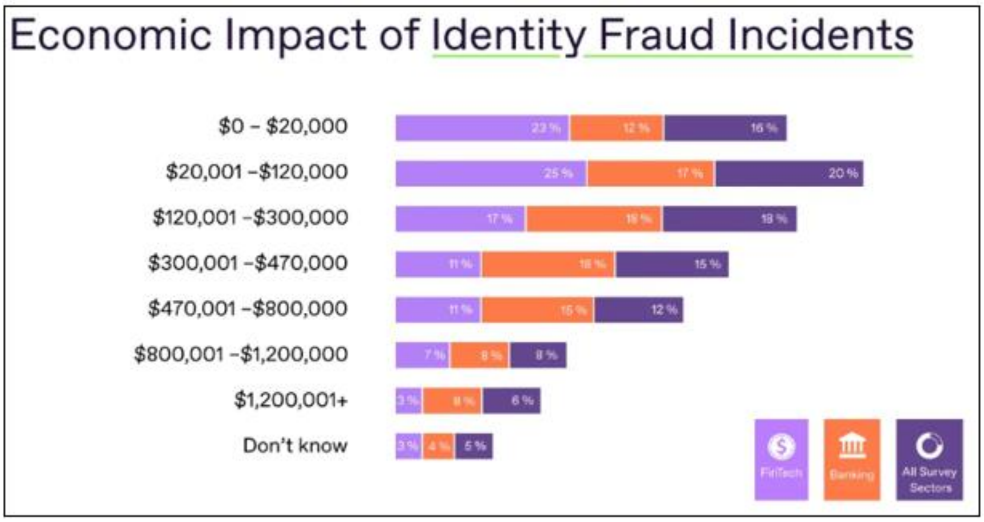



[5]

**Fraud**

Know Your Customer (KYC) practices are becoming more and more important as identity fraud poses a growing threat to the financial services sector. According to recent results from a global assessment by Regula and Sapio Research, in 2022 over 100 identity fraud occurrences occurred in every fourth bank, with a median financial cost exceeding $310, 000. [6] According to a Regula global survey, 26% of banks reported more than 100 identity fraud instances in the previous year, and 31% of banking organisations experienced a financial cost of at least $479, 000. [6]

A rising issue is emerging risks, such deepfake video fraud, which 79% of leaders think could seriously harm their companies. [6]




[6]



Paper ID: SR24517175239 DOI: https://dx.doi.org/10.21275/SR24517175239

## 4. Solutions

Fintech companies can lower excessive expenses by using AI to automate procedures, outsourcing non - core work, negotiating better prices with suppliers, and streamlining internal operations. Effective cost management also involves using scalable solutions and keeping a careful eye on expenditures. AI - powered process automation simplifies KYC, cutting down on human mistake and saving time. Verification is a work that experts may undertake effectively through outsourcing.

Fintech companies can use AI for database searches and document verification to speed up KYC procedures quickly and affordably. AI and outsourcing help streamline KYC procedures, which lowers the number of customers who leave. Proactive support and streamlined verifications reduce frustration. Optimising resource allocation using scalable systems and risk - based techniques guarantees seamless onboarding. Negotiated pricing and open - source technology reduce expenses while maintaining customer satisfaction and loyalty.

Lastly, Fintech companies can invest in advanced identity verification technology like biometrics and AI - driven facial recognition to fight identity fraud, including new threats like deepfake video fraud. Risks can be reduced without incurring significant costs by working with industry professionals to develop affordable solutions, putting strong fraud detection algorithms into place, and informing clients about security precautions.

## 5. Conclusion

To maintain compliance and confidence in the financial industry, KYC is a vital component in the battle against financial crimes. Fintech businesses are using AI and biometrics to improve security and expedite procedures despite obstacles like expense and fraud. Through adopting creative ideas and proactive tactics, these companies promote financial inclusion while adhering to regulations. The industry can protect itself against new risks like deepfake fraud by investing in cutting - edge technologies and adapting continuously. This will ensure a strong and stable financial environment for all parties

## References

[1] Concentrix. “KYC in Fintech: Tackling the 3 Biggest Challenges” [Online]. Available: Webhelp. com | Articles | KYC in Fintech: Tackling the 3 Biggest Challenges
[2] Persona. “Why does KYC matter for Fintech companies” [Online]. Available: KYC for Fintech: Importance & Challenges | Persona (withpersona. com)
[3] International Telecommunication Union. “e - KYC use case in digital finance” [Online]. Available: e - KYC - innovations - use - cases - in - digital - financial - services. pdf (itu. int)
[4] Dojah. “The History for KYC” [Online]. Available: The History of KYC (dojah. io)
[5] Public Investment Fund. “Fintech and e - money customer onboarding benchmarking report” [Online]. Available:
[6] PIF_Whitepaper_Fintech_and_Emoney_Benchmarking_report. pdf (hooyu. com)
[7] Regula. “Automated KYC Verification Guide: How to Fight Fraud and Improve Compliance” [Online]. Available: How Automated KYC Verification Transforms Client Compliance (regulaforensics. com)