PCI PAYMENTS COUNCIL OF INDIA   IAMAI Internet And Mobile Association Of India   FCC Fintech Convergence Council

White Paper on Digital KYC Solutions

Submitted by:

Internet and Mobile Association of India (IAMAI)

Payments Council of India (PCI)

Fintech Convergence Council (FCC)

Table of Contents

1. Background and Context

In FY 2017-18, the Services sector contributed almost 72.5%[1] to India's Gross Value Added (GVA) growth, of which the Financial Services[2] sector contributed 7.3%. Financial Services sector has, in recent years, been focused on developing an inclusive society, by creating last mile reach and developing new-age business model, aided by technology, to ensure basic financial services are provided to the underserved population. In order to ensure a financially inclusive society, great emphasis has been laid on KYC procedures, especially for residents in remote areas of the country.

KYC procedures are measures taken by regulated entities, to identify and verify their customers, prior to transacting or establishing an account-based relationship with them. Such identification helps business entities to understand their customers and their financial dealings, thereby reducing the likelihood of money laundering activities and terrorist financing. In India, the subject of permissible KYC processes has been a matter of great discussion across the stakeholders – Government, regulators, entities and customers.

In recent years, the financial services industry has been grappling with challenges in respect of performing KYC verification of its customers, in light of the recent Supreme Court judgement and given the lack of common standards and solutions for KYC. Thus, the financial services industry, under the aegis of Internet and Mobile Association of India, Fintech Convergence Council and Payments Council of India, has come together to explore alternatives for KYC that may be adopted by any financial service provider, across sectors. In various sessions, industry participants have put forth suggestions and deliberated the merits/demerits of various alternatives for KYC.

This paper outlines the evolution of the KYC regulatory framework in India in the pre-Aadhaar, post-Aadhaar era and the current scenario; and articulates the industry's efforts towards, collectively, developing an alternative framework for KYC verification (in addition to the existing paper-based and offline Aadhaar process) which would include critical aspects such as potential digital solutions for face-to-face and remote KYC verification, risks pertaining to the identified solutions, safeguards to address the risks, and economic viability of the alternative solutions. Further, the industry has mutually agreed upon and provides recommendations on key features or principles that should be intrinsic to any KYC solution, requisite amendments to the extant regulatory framework, in line with the needs of the industry and other alternative solutions which may be considered by the authorities, as a long-term solution to address the KYC needs of the industry.

[1] Source: Economic Survey 2017-18

[2] Also includes Real estate, ownership of dwelling & professional services

2. Evolution of the KYC Regulatory Framework in India

The Prevention of Money Laundering Act, 2002 (PML Act) is the governing legislation in India for aspects concerning money laundering and terrorist financing. The PML Act and Rules framed thereunder require reporting entities to perform specific activities, such as client due diligence, maintenance of records, suspicious transaction reporting etc. to mitigate the risk of money laundering and terrorist financing. As per the provisions of the PMLA, every financial institution (including banks, NBFCs, PPIs, insurance companies, SEBI/IRDA registered intermediaries) is required to follow client due diligence procedures and maintain records of such transactions, as prescribed by the Act and rules notified thereunder. Rule 9 of the PML Rules provides the governing framework for client due diligence procedures and standards to be adopted by reporting entities

The financial services industry is largely regulated by its three regulators viz. IRDAI, RBI and SEBI; and hence the policy framework regarding AML and CFT is developed by the respective regulators, in line with the tenets of the PML Rules. The fundamental obligation of reporting entities, iterated by all three regulators, is to establish the identity of the client and obtain information pertaining to the nature of business. To enable this, the regulators have prescribed certain officially valid documents that may be obtained from the customer, to satisfy as proof of identity and proof of address.

The regulators also provide KYC norms against which, verification procedures are to be put in place by every reporting entity, to verify the document/ information proofs that have been submitted by customers. Accordingly, KYC verification was, in the past, performed using two methodologies – a) obtaining ‘certified copy’ of an OVD i.e. comparing the original OVD with the copy produced by the customer (known as ‘original seen and verified’ or ‘OSV’ in industry parlance), and b) in-person verification, as has been prescribed in SEBI guidelines.

The ensuing section details the evolution of the KYC regulatory framework over the last decade, classified as the pre-Aadhaar era, post-Aadhaar era and the current scenario (post Supreme Court judgement).

2.1. Pre-Aadhaar Era

Rule 9(1) of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 requires reporting entities to identify its clients, verify their identity, obtain information on the purpose and intended nature of the business relationship, at the time of establishing an account-based relationship. Further, it also provides that where the client is an individual, he shall for the purpose of sub-rule (1), submit to the reporting entity, **one certified copy of an ‘officially valid document’ containing details of his identity and address, one recent photograph** and such other documents including in respect of the nature of business and financial status of the client as may be required by the reporting entity.

The financial services regulators (RBI, SEBI and IRDA) adopt the aforesaid framework and issue specific directions to their respective regulated entities for compliance. Noted below are certain additional instructions issued by each of the regulators that are relevant in the context of conducting customer due diligence.

RBI	SEBI	IRDA
○ Regulated entities shall ensure that no account is opened in anonymous or fictitious/benami name ○ No account is opened where the Regulated entity is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/ information furnished by the customer ○ While considering customer's identity, the ability to confirm identity do`cuments through online or other services offered by issuing authorities may also be factored in Regulated entities shall ensure that the first payment is to be effected through the customer's KYC-complied account with another regulated entity, for enhanced due diligence of non-face to face customers ("Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the regulated entities or meeting the officials of regulated entities).	○ Verify the client's identity using reliable, independent source documents, data or information ○ In-person Verification (IPV) of clients must be mandatorily carried out by all SEBI registered intermediaries ○ To avoid duplication of KYC process with every intermediary, KRA mechanism having centralized KYC records needs to be followed.	Any document that is accepted by the entity should be such that it would satisfy regulatory / enforcement authorities, if need be at a future date that due diligence was in fact observed by the company in compliance with the guidelines and the PML Act.

Paper-based KYC verification

In the pre-Aadhaar era, paper-based KYC verification was adopted by service providers across industries for customer onboarding and due diligence measures. Service providers accepted any of the Officially Valid Documents (as listed below), for establishing identity and address of a customer. Further, based on the sectoral guidelines prevalent in the economy, service providers deployed a network of agents to perform in-person verification and OSV of KYC documents. Such measures of customer onboarding was very expensive and took nearly 3-5 days for completion of the customer's due diligence.

List of Documents accepted for KYC verification

- Passport
- PAN Card (Proof of Identity only)
- Driving License
- Voter ID Card issued by Election Commission of India

2.2. Post Aadhaar Era

In 2009, the Unique Identification Authority of India (UIDAI) was established as an attached office of the then Planning Commission (now NITI Aayog). UIDAI was established with the purpose of issuance of a Unique Identification number or 'Aadhaar' to the residents of India. The Aadhaar was envisaged to be robust enough to eliminate duplicate or fake identities and to be verified and authenticated in an easy and cost-efficient manner. Gradually, Aadhaar card/letter issued by UIDAI was recognised as an acceptable OVD for the purpose of KYC, through a notification issued on 16th December 2010. In addition, job card issued by NREGA (duly signed by an officer of the State Government Government/ Defence ID Card) was also accepted as an OVD.

In 2016, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act 2016") was passed by the government. The success of the Aadhaar framework was evident is its mass penetration across the country and rapid adoption by the service providers across the financial services industry. Aadhaar OTP based KYC was a seamless customer verification measure introduced by UIDAI, by virtue of which service provides could authenticate customers using their Aadhaar number and could provide services to such customers for a period of 12 months, pending complete biometric-based eKYC verification. Thereafter, in 2017, customer due diligence based on Aadhaar-eKYC was made mandatory under the PML Rules. Accordingly, service providers in the country made significant investments to establish the requisite infrastructure for Aadhaar based eKYC authentication and, for some, to obtain the requisite licence from UIDAI.

Supreme Court Verdict on Aadhaar Framework

The recent Supreme Court verdict on the Aadhaar framework, pronounced on 29th September 2018, rendered a part of Section 57 of the Aadhaar Act, which enabled private entities to use Aadhaar for establishing the identity of an individual, unconstitutional. The Supreme Court observed that this section was read down to mean that use of Aadhaar by private entities was for any purpose 'backed by law' or contract to that effect. The Court stated that such provision does not meet the proportionality test for want of judicial scrutiny. Thus, private entities can no longer use Aadhaar based eKYC for authentication purpose, other than for welfare schemes such as DBT.

Additionally, the Supreme Court also struck down specific amendments to Rule 9 of the PML Rules which mandated linking of a customer's Aadhaar number with his/her bank account. In light of the said judgement, there remains much uncertainty in the permissible KYC procedures that can be adopted by service providers in the country.

2.3. Current Scenario

In the absence of any changes in the sectoral regulations post-SC judgement, several industry players are resorting to paper-based KYC verification. Reverting to such procedure is at the expense of customer convenience, turnaround time and cost-optimisation.

It is pertinent to note that the state of KYC infrastructure in the country, today, is lagging in comparison to the Aadhaar framework. While there are four alternative officially valid documents available for performing KYC of an individual, the technological infrastructure is inadequate for service providers to be able to authenticate the identity of the individual by accessing the respective database.

To illustrate this, one may consider the voter ID which is considered the most pervasive OVD in the country, after Aadhaar. While voter IDs are registered on a national database, retrieval of customer records pertaining to an Electoral Photo Identity Card (EPIC) number highlights, merely, the voter's name, gender, father's name and polling station details - grossly deficient in providing critical details such as the photograph of the voter and the address. Similarly, there are inadequacies in the details that can be obtained from databases of other OVDs such as PAN, Driving License and the Passport.

List of proofs provided by OVDs				
	Officially Valid Documents			
Documents/ Parameters	**PAN**	**Driving license**	**Voter ID**	**Passport**
Database	NSDL	Parivahan	Electoral Search (National Voters' Search Portal)	NA
Input fields by customer	PAN Number	DL No.	EPIC No.	Image of Passport
	Name on PAN card	DOB	Elector's Name	Name
Photograph				
Photo Match	No photo generated	No photo generated	No photo generated	NA
Proof of Identity				
Name	Verified	Not Verified	Verified	Name provided by customer verified against passport
DOB	Verified	Not Verified	Verified	Extracted
Proof of Address				
Current/Permanent address	Address not available	Available in ID	Available in ID	Available in ID

Amendments to Legal Framework

Amendment to The Prevention of Money Laundering (Maintance of Records) Rules, 2005

On 13th February 2019, the Department of Revenue issued a notification, amending the PML Rules. The amendments provide for the acceptance of "proof of possession of Aadhaar number" as an OVD, in such form as issued by UIDAI. With this, the government seemingly enabled the use of Aadhaar Offline (XML) and Aadhaar secure QR code as a means of identification. However, the use of Aadhaar-based eKYC continues to be facilitated only for the purpose of welfare/subsidy schemes by Banks.

The Aadhaar and Other Laws Ordinance, 2019

On 28th February 2019, the **Aadhaar and other Laws (Amendment) Ordinance, 2019** ('Ordinance') was approved by the President. The Ordinance amended the Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016 and Prevention of Money Laundering Act, 2002. The Ordinance provides for voluntary use of Aadhaar number, in physical or electronic form, by way of authentication or offline verification by Banks. The Ordinance does not enable regulated non-bank entities other than banks to use the Aadhaar eKYC framework for authentication. Amendments to the PMLA, brought by the Ordinance, enable the government to permit a reporting entity (other than Banks) to perform Aadhaar-based authentication, if it is satisfied that such reporting entity complies with the standards of privacy and security specified under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, and if it necessary and expedient to do so.

Further, the amendment enables the use of Aadhaar offline for customer due diligence, however, does not provide any relief to service providers, in terms of the methods for generation of the respective e-Aadhaar and XML file by customers. It is an unsurmountable task to make the customers, especially in the semi-urban and rural areas, to generate the XML file/ e-Aadhaar from the UIDAI website, without any service provider intervention.

2.4. PAN Mandate

The PML Second Amendment Rules also mandated obtaining a customer's Permanent Account Number or Form 60. Given that the penetration of PAN is lacking, in the country, this became an uphill task for regulated entities. While the government's intent is appreciated in mandating PAN for performing customer KYC, obtaining Form 60 from the larger population in the country has been a cumbersome task, given how the document is available in physical form only.

3. Digital KYC - Potential Alternative Solutions

In this section, the proposed digital solutions for customer onboarding are outlined. The solutions are classified based on the customer interface for initiation of onboarding viz. face-to-face and remote onboarding.

3.1. Face-to-Face solutions

Face-to-face KYC verification occurs at the premises of a service provider/ authorised BC and necessitates the presence of, both, the business correspondent and individual (customer). Customer onboarding in a face-to-face method shall fulfil RBI's regulatory requirement of obtaining a certified copy of OVD from customer i.e. comparing the copy of OVD produced by the customer with the original and recording the same on the copy (OSV) by the authorised officer of the service provider. The risk involved in such scenarios are inherently lower than remote onboarding (non-face-to-face) and can thus lend itself to technology-based implementation.

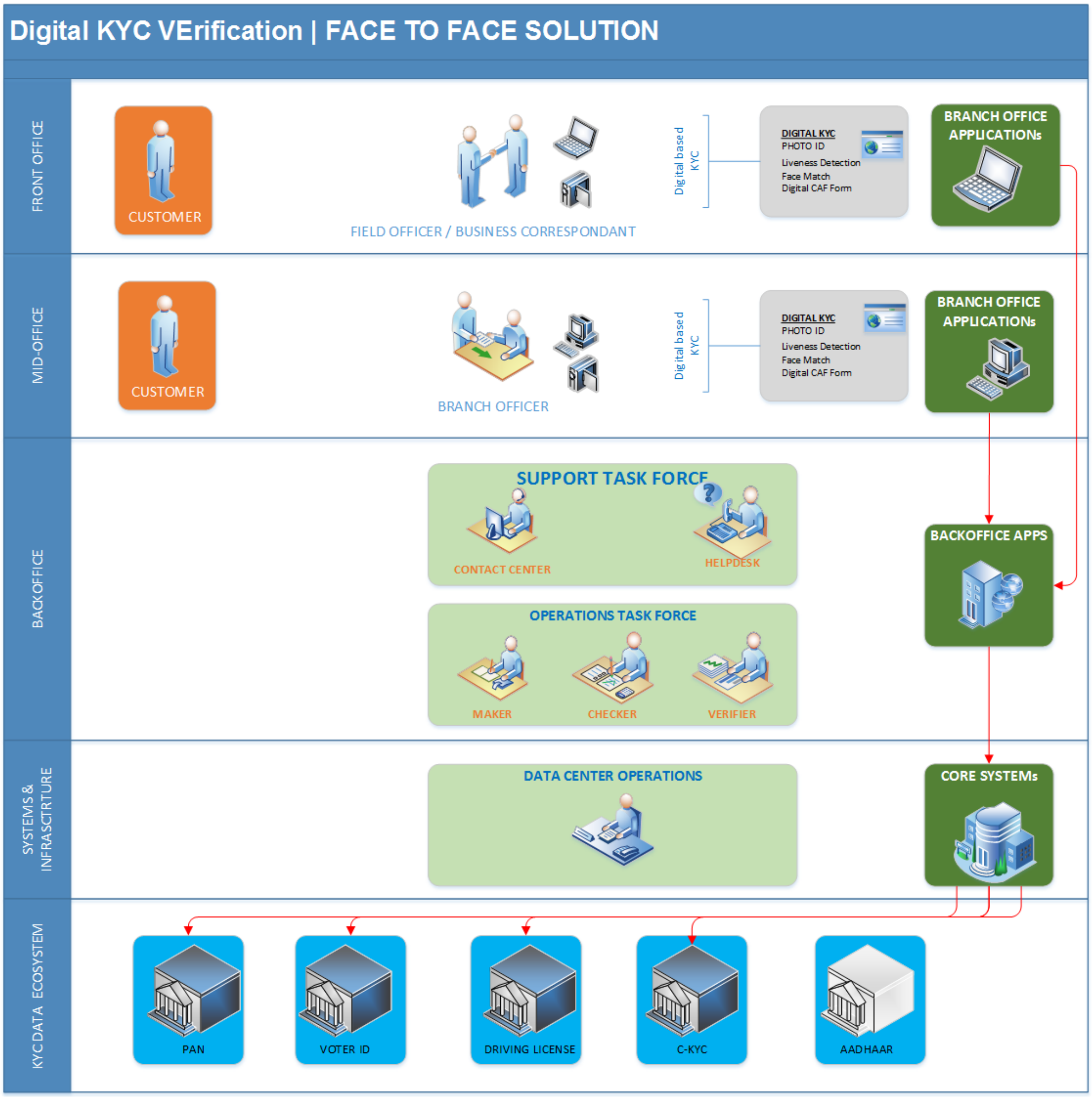
Process Flow

The process for face-to-face customer onboarding using technological means would involve the following steps.

1. Authorised agent/ BC at the premises to authenticate himself on the agent system before every transaction
2. Agent/BC to obtain customer consent for initiation of customer onboarding
3. Customer to fill the Customer Acquisition Form in the presence of the agent; BC to have limited control over the data being filled in the form
4. Agent/ BC to capture a live image of the original OVD document provided by the customer. BC will not have an option to upload an image from gallery. At the back-end, system will perform the following checks:
    a. Verification of authenticity of the customer ID image; Alternately OVD details to be validated against Government/ Issuing agency database(s) if interfacing feasibility is available
    b. Matching of details in Customer Application Form against OVD
5. BC to capture a live image/video of the customer and authenticate the customer. At the back-end, system will perform the following checks:
    a. Liveness detection of the captured photograph/video
    b. Captured photo should be clear and meet basic standards (eyes not closed, not over exposed etc.)
    c. Face match of the live customer image with the photo on the ID card[3]

[3] Studies indicate that machines are superior to humans in terms of face comparison https://www.researchgate.net/publication/244988572_Comparing_Face_Recognition_Algorithms_to_Humans_on_Challenging_Tasks

The above process flow aims to reduce/eliminate any risk of fraud that may arise during a face-to-face customer onboarding process, by way of technology-aided verification and controls.



Author – Prasanna Lohar , DCB Bank

3.2. Remote solutions

Remote solution involves onboarding of customer in the absence of physical contact with the customer. Such scenarios entail higher risk of fraud, hence necessitate robust checks and controls for customer due diligence and verification.

Process

The process for face-to-face customer onboarding using technological means would involve the following steps.

1. Customer to fill the Customer Acquisition Form and provide consent for initiation of onboarding process
2. Customer to capture a live image of the OVD document; Customer will not have an option to upload any image from gallery. At the back-end, system will perform the following checks:
    a. Verification of authenticity of the customer ID image by detection of holograms, optical variable ink and other security characteristics in the OVD; OVD details to be validated against Government/ Issuing agency database(s)
    b. Matching of details in Customer Application Form against OVD using the following tech-based solutions:
        i. OCR based automated data capture and form filing from multiple documents
        ii. Document validation and consistency check based on MRZ analysis
    c. OVD details to be validated against Government/ Issuing agency database(s)
3. Customer to capture a live image/ video of self. At the back-end, system will perform the following checks:
    a. Liveness detection of the captured photograph/video using 3 dimensional facial analysis (For example, rather than detection of basic liveliness gestures such as blinking of eyes or smiling i.e. gestures which include movement, a holistic liveliness detection technique which creates a 3D model of the face and detects suspicious “dimensioning” of features such as the jaw will be deployed)
    b. Captured photo should be clear and meet basic standards (eyes not closed, not over exposed etc.)
    c. Face match of the live customer image with the photo on the ID card
    d. Algorithms that are specifically trained to recognize spoofing attacks to be in place.
4. At the back-end, *Post facto* manual review of customer information will be performed, on a periodic basis. Authorised officer will sign-off on the customer verification (akin to OSV)

Fraud Control Measures

- No notification to customer during onboarding about security check results (e. g. hologram check failed or face recognition failed) to deter misuse and/ or attack on system.
- Checks and data extractions to occur at the back-end and not on mobile phone/web browser itself.
- Transfer of verified data from the backend to the frontend (e. g. mobile phone) to be avoided so as to prevent any data leakage

3.3. Economics of Digital KYC

Any KYC solution that is deployed must be economically viable in order to be widely adopted. This section explores the cost component of KYC deployment. Cost of KYC varies dramatically depending on the context that it used. Here are some of the contexts that we have explored in order to come up rough estimates of cost.

1. **KYC at a Branch -**
    a. Branch sign ups have historically happened using paper based form filling methods. This is the preferred method for most banks in India. Even though branches collect paper, the actually digitisation of paper typically happens in centralised data processing centres. The cost drivers in such cases tend to be in (1) printing paper, (2) transcribing written forms in order to enter them into core banking systems and (3) courier costs. This method of sign up actually takes 7 to 10 days in most cases

    b. Lately banks have adopted eKYC to help digitise the process. Paper forms can be completely eliminated in this process. The cost drivers in this case are (1) biometric device costs, (2) transaction costs for every eKYC and any license (such as AUA fees) and maintenance costs for the software platform used for eKYC

    c. This whitepaper advocates a digital KYC journey for the branch use case. This can eliminate costs related to printing, transcription and courier. However digital solutions have associated charges typically expressed as a per user sign up charge
2. **KYC using small retailers -**
    a. This journey originally pioneered by telecom companies to sign up new users, has been exploited by payments and remittances players too. It is also a very significant channel for payment banks. Historically this channel has utilised biometric based eKYC to sign up users and so the cost drivers have been (1) agency charges that typically go the small retailer, (2) maintenance / replacement of biometric devices as well as (3) eKYC transaction costs and any license (such as AUA fees) and maintenance costs for the software platform used for eKYC. An important risk, flagged by Supreme Court as well as UIDAI, has been the uncontrolled use of biometric devices by independent retailers

    b. Digital KYC journey can be easily rolled out to a wide spectrum of retailers. The risk of access to sensitive data using biometric devices is effectively mitigated in this scenario. The cost driver in this case would be (1) agency charges by the small retailer as well as (2) the software charge associated with the digital KYC solution
3. **KYC using runners (Feet on Street)**
    a. Traditionally this type of KYC has been a standard feature of the lending use case. Runners have collected KYC papers along with other forms required for the specific use case. The cost drivers include (1) charges per pick up of documents (runner fees) and (2) charges associated with paper printing, courier, transcription and storage

    b. Lately runners have also been armed with biometric devices. This speeds up the sign up journey considerably. However it also adds the risk of uncontrolled usage of biometric devices by 3rd party personnel. The cost drivers in this case would be (1) runner fees, and (2) eKYC transaction costs and any license (such as AUA fees) and maintenance costs for the software platform used for eKYC

    c. Digital KYC solutions can also be easily deployed to a fleet of runners. This mitigates the risk of uncontrolled access to sensitive data using biometric devices. The cost associated with this solution would be (1) runner fees, and (2) the software charge associated with the digital KYC solution

4. **Remote KYC -**
    a. Within limitations of eligibility (restricted timelines, capped amounts etc), OTP based eKYC has been used for end user sign up. Here the cost driver is primarily the eKYC transaction costs and any license (such as AUA fees) and maintenance costs for the software platform used for eKYC
    b. In a similar way digital KYC may also be adopted for remote sign ups.

Comparison of User Registration costs across channels

Channel for User Sign up	**Total (Per User)**	eKYC	Digital KYC	Biometric Device	Retail Agents	Runner	Printing, Transcription, Courier, Storage
Branch Biometric	7.04	6.00	-	1.04	-	-	-
Branch Paper	120.00	-	-	-	-	-	120.00
Branch Digital	25.00	-	25.00	-	-	-	-
Retail Biometric	77.04	6.00	-	1.04	70.00	-	-
Retail Digital	95.00	-	25.00	-	70.00	-	-
Runner Biometric	407.04	6.00	-	1.04	-	400.00	-
Runner Digital	425.00	-	25.00	-	-	400.00	-
Runner Paper	520.00	-	-	-	-	400.00	120.00
Remote eKYC (OTP)	6.00	6.00	-	-	-	-	-
Remote Digital	**25.00**	-	25.00	-	-	-	-

Assumptions for estimating costs

1. For the purpose of calculations we have assumed that 50,000 users would be signed up in a month
2. Where applicable we have assumed that about 1000 biometric devices would be used and that biometric devices cost approximately INR 2500
3. We have assumed that AUA licenses charges and maintenance of the platform for eKYC would cost rough INR 3,000,000 per year
4. We have assumed that eKYC transaction charges are INR 1 per transaction and Digital KYC charges are INR 25 per user
5. We have assumed that charges retailer would charge INR 70 per sign up and that runner would charge INR 400 per sign up
6. We have assumed that printing, courier, transcription and storage would cost INR 120

4. Our Recommendations

With the evolution of the global economy and technological advancements, the trends in consumer services, especially in the financial services segment have been changing accordingly. Accordingly, standards of banking, payments, KYC, fraud prevention etc. have also evolved. To keep with the changing industries and technologies, Asian jurisdictions such as Singapore, Hong Kong, Thailand, Indonesia and Malaysia have adopted a risk based approach for policy making, particularly in terms of KYC, with certain countries permitting non-face-to-face customer onboarding, provided the risks are adequately managed by the service providers.

Keeping with global norms, for any digital KYC solution to be acceptable to the stakeholders involved, there should be specific standards and principles which will fulfil the regulatory, security and social (accessibility and ease of use) requirements. This section outlines the fundamental principles, minimum criteria/ features that should be embedded into a digital KYC solution to ensure that it mitigates the risks (fraud, IT etc.) associated with the use of the solution. Our recommendations herein shall be successful only if they are in consonance with the applicable regulatory provisions. Hence, we have highlighted the necessary amendments in existing laws and regulations that the government and regulatory authorities may consider for implementation of the proposed Digital KYC Solutions.

4.1. Key Principles

The Digital KYC solutions envisaged to be implement should exhibit the following recommended principles, which will be instrumental in designing the features of such Digital KYC solution.

1. **To effectively identify the user**
2. **To authenticate the user**
3. **To be available and scalable**
4. **To be safe and secure**
5. **Face Recognition (liveliness check)**
6. **To establish accuracy of data**

It is envisaged that the aforesaid principles shall be reflected in the features of the Digital KYC Solutions, as enlisted in the ensuing section.

It is important to highlight, however, that Digital KYC solutions should be seen in conjunction with other forms of KYC and in relation to the risk associated with the associated transaction. An illustration of this is the use of OTP-based eKYC (prior to the SC judgment) for low risk transactions and the application of a limited validity period for availing of services by the respective customers.

Keeping with the fundamental principle of FATF, we also recommend in the ensuing sections, a risk-based approach for the use of Digital KYC solution.

4.2. Minimum Criteria/ Features of Digital KYC Solution(s)

The following table outlines the recommended minimum criteria / feature list for acceptance as a Digital KYC solution.

Category	Features	Description
General	**Geolocation**	This is the geolocation of the user at the point of the digital KYC transaction. Capturing the geolocation of the transaction leads to transparency and auditability
	Timestamp	This is the timestamp taken on the completion of transaction for digital KYC
	Consent	The user is required to consent to giving his data for the purpose of KYC to both the data processor and the data controller
ID Checks	**Document Validation**	This is act of determining that the ID card presented is genuine on the basis of its physical properties
Authentication	**Face Match**	This is the act of comparing a photograph of the user against the photo on his/her ID card
	Liveness	This is the act of determining if the user was present at the time of transaction
IT Security	**At Rest Encryption**	The minimum requirement for encryption at rest is AES 56
	Network Encryption	SSL is a basic minimum requirement for the network used for transmitting data required for Digital KYC
Data Security	**Sovereignty**	Processing and storage of data to be in India. Data will be auditable at each step.

While the above features are recommended, it is critical to ensure that the features satisfy the regulatory requirements prescribed under the PMLA framework and the guidelines issued by the respective regulators, as explained through the compliance followed under paper-based KYC.

Category	Paper-based KYC (current process)	Digital KYC (proposed process)	Additional comments
General	• Consent is typically taken as part of Customer Application Form • Company's Authorised Officer signs and puts a date and place to record the OSV process	• Customer consent will be taken • Geolocation of the process is captured • Timestamp of process is captured	Digital approach ensures more transparency and auditability with scope for controls

OSV	• Authorised Officer **compares** original OVD with photocopy	• System determines genuineness of OVD based on physical properties • Supports all OVDs • OVD should be certified using digital signature of Authorised Officer of RE	Digital approach can include reliable database checks for additional controls
Photo Match	• Authorised Officer meets user **face to face**	• Video-identity & Liveness test determines customer's presence	
	• Authorised Officer **compares** ID against face	• Compares photo of the customer against the photograph on OVD	
IT Security	• **No defined standards**	• Encrypt at Rest – All stored data should be encrypted	
	• **No defined standards**	• Encryption (SSL) to be used for all transmissions	

4.3. Amendments to regulatory framework

In line with the principles and parameters set out above, we recommend inclusion of the following aspects in the PMLA framework and KYC regulations issued by the respective regulators:

i) Reporting Entities (REs) may rely on reliable information technology system as the tool for verifying the identity of the customer

ii) REs may use technological means such as video calls for photo validation/ liveliness check of the customer

iii) Presently, the financial services regulators – RBI, SEBI and IRDAI, each prescribes KYC measures through its respective guidelines. However, there is a dire need to also standardise the regulations across sectors, so as to ensure efficiency in the KYC process adopted by service providers across segments.

iv) To allow non-bank entities to access and use eKYC authentication framework. The recent amendments in the PMLA and the Ordinance, both, do not enable non-bank entities to participate in the Aadhaar framework. The industry recognises the concerns of the Supreme Court vis-à-vis security of customer information and Aadhaar data, and assures to comply with the security requirements prescribed by UIDAI

4.4. Establishing a Centralised KYC Repository

Vide notification dated July 7, 2015 amending the PML Rules, the government introduced a plan to set up the Central KYC Records Registry (CKYCR). The CKYCR was proposed to serve as a repository to receive, store, safeguard and retrieve KYC records in digital form of a client (individual). The KYC records received and stored by the CKYCR could be retrieved online by any reporting entity across the financial services industry for the purpose of establishing an account-based relationship with a customer. The CKYCR is managed by Central Registry of Securitisation Asset Reconstruction and Security Interest (CERSAI).

Since launch, the CKYCR has been plagued with technical and operational issues. Despite several attempts, industry players have faced multiple glitches in its operations which has affected its accessibility and is an impediment to the operational journey for service providers.

In light of the existing challenges associated with the CKYCR, we recommend development of a centralised KYC repository called the KYC bureau which would be setup by an independent private body, duly representing the interests of the financial services industry. The body shall invite membership from all the relevant participants such as banks, NBFCs, PPI companies, and entities registered with SEBI/IRDAI etc KYC bureau would also invite existing bureaus like SEBI registered KRAs, Credit bureaus etc to share the existing KYC data. Members will be enabled to share/upload and access KYC data of their customers as per the standards prescribed by the body and agreed by the members. Each customer will be assigned a unique customer id to indicate the KYC records pertaining to him/her. Similar to the CKYCR process, customers can share their customer id with other member service providers, to reduce and eliminate providing KYC documents repeatedly, thus enabling efficiency in the KYC process and cost-optimisation for the financial services industry.

5. Glossary of Terms

Sr. No.	Term	Meaning
1.	AML	Anti-money laundering
2.	AUA	Authentication User Agency
3.	BC	Business correspondent
4.	CAF	Customer Acquisition Form
5.	CDD	Client Due Diligence
6.	CERSAI	Central Registry of Securitisation Asset Reconstruction and Security Interest
7.	CFT	Counter terrorist financing
8.	CKYCR	Central KYC Records Registry
9.	DBT	Direct Benefit Transfer
10.	EPIC	Electoral Photo Identity Card
11.	FATF	Financial Action Task Force
12.	FCC	Fintech Convergence Council
13.	IAMAI	Internet and Mobile Association of India
14.	IPV	In-person verification
15.	IRDAI	Insurance Regulatory and Development Authority of India
16.	KRA	KYC (Know Your Client) Registration Agency
17.	KYC	Know Your Customer
18.	MRZ	Machine Readable Zone
19.	NREGA	National Rural Employment Guarantee Act, 2005
20.	OCR	Optical character recognition
21.	Ordinance	Aadhaar and other Laws (Amendment) Ordinance, 2019
22.	OSV	Original seen and verified
23.	OTP	One-time password
24.	OVD	Officially Valid Document
25.	PCI	Payments Council of India
26.	PML Rules	Prevention of Money-laundering (Maintenance of Records) Rules, 2005
27.	PMLA	Prevention of Money Laundering Act, 2002
28.	RBI	Reserve Bank of India
29.	SEBI	Securities and Exchange Board of India
30.	UIDAI	Unique Identification Authority of India