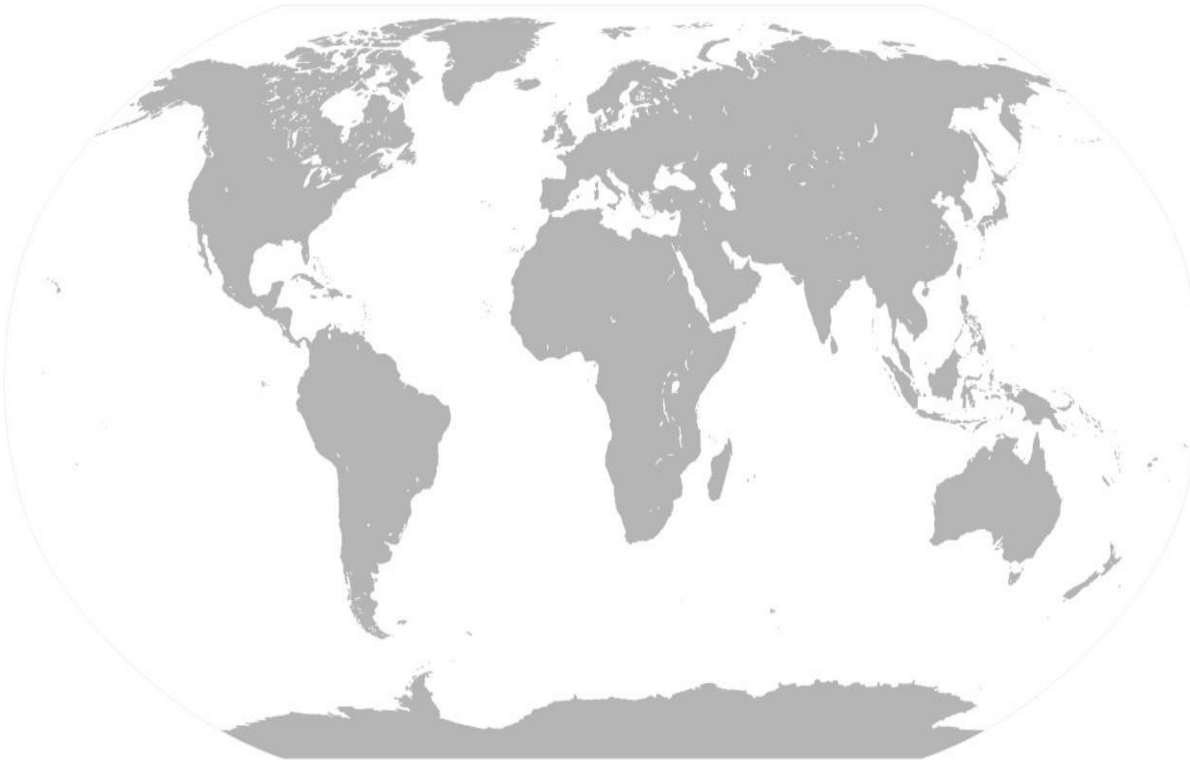
Amicus
Transcending Frontiers



The waxing and waning of digital KYC processes

JUNE 17, 2020

E-mail: info@amicusservices.in
Website: www.amicusservices.in

The waxing and waning of digital KYC processes

Why is KYC required?

'Know your customer', compliance lies at the core of establishment and verification of identity of the customers by regulated institutions. While the regulatory objective of KYC is to prevent money laundering, KYC procedures also enable Reporting Entities to know and understand their customers and manage their risks prudently. The statutory framework for KYC regime is provided by Section 11A of the Prevention of Money Laundering Act, 2002[1]("**PMLA**"), which requires banking company, financial institution, intermediary or a person carrying on a designated business or profession ("**Reporting Entities"**) to verify the identity of their clients. However, sector specific regulators, such as Reserve Bank of India, Securities and Exchange Board of India and Insurance Regulatory and Development Authority of India have established their own detailed KYC guidelines for Reporting Entities which are regulated by them.

In this article, we discuss the evolving landscape of the KYC Guidelines issued by Reserve Bank of India ("**RBI**") from time to time, which has often been impacted by seismic changes such as the Aadhar judgment of the Supreme Court and the more recent COVID-19 pandemic.

[1] 11A. (1) Every reporting entity shall verify the identity of its clients and the beneficial owner, by--
(a) authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016) if the reporting entity is a banking company; or
(b) offline verification under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
(c) use of passport issued under section 4 of the Passports Act, 1967 (15 of 1967); or
(d) use of any other officially valid document or modes of identification as may be notified by the Central Government in this behalf:
Provided that the Central Government may, if satisfied that a reporting entity other than banking company, complies with such standards of privacy and security under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and it is necessary and expedient to do so, by notification, permit such entity to perform authentication under clause (a):
Provided further that no notification under the first proviso shall be issued without consultation with the Unique Identification Authority of India established under sub-section(1) of section 11 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016) and the appropriate regulator.
(2) If any reporting entity performs authentication under clause (a) of sub-section (1), to verify the identity of its client or the beneficial owner it shall make the other modes of identification under clauses (b), (c) and (d) of sub-section (1) also available to such client or the beneficial owner.
(3) The use of modes of identification under sub-section (1) shall be a voluntary choice of every client or beneficial owner who is sought to be identified and no client or beneficial owner shall be denied services for not having an Aadhaar number.
(4)If, for identification of a client or beneficial owner, authentication or offline verification under clause (a) or clause(b)of sub-section(1)is used, neither his core biometric information nor his Aadhaar number shall be stored.
(5) Nothing in this section shall prevent the Central Government from notifying additional safeguards on any reporting entity in respect of verification of the identity of its client or beneficial owner.
Explanation.-- The expressions "Aadhaar number" and "core biometric information" shall have the same meanings as are respectively assigned to them in clauses (a) and (j) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).]

A brief flashback

Aadhaar and the technological stack developed around it was a game- changer for the KYC process. Aadhaar as an officially valid document was already being used since 2010, but it was between 2016 and 2018 that KYC (through Aadhaar) was at its most simplified and digital form. This was the time when Aadhaar based e-authentication was allowed as part of KYC. There were various types of Aadhaar based e-authentication that were being utilised for KYC: yes/no authentication, where Central Identities Data Repository (CIDR) checked whether the data submitted matches with the data available with the CIDR or not and replied with a yes or no; OTP or biometric based authentication whereby biometric information and/or OTP and Aadhaar Number submitted was matched against the data available in the CIDR, and the Unique Identification Authority of India (UIDAI) returned a digitally signed response containing e-KYC data. Moreover, subject to certain conditions, accounts were allowed to be opened in non- face to face mode i.e. customers could open accounts without visiting the branches/offices of the RE's or meeting the officials of RE's. The availability of a presence-less and paperless mode of undertaking KYC through Aadhar and the Indiastack developed around the Aadhar infrastructure not only eased KYC processes but also spawned a host of fintech innovations and businesses, which used Aadhar based e-KYC as a voluntary and expeditious mode of undertaking KYC.

However, during the same time, given the lack of robust privacy laws in India, the Aadhaar framework also came under legal challenge before the Supreme Court of India for breach of privacy and as a tool that had potential for being used by government for surveillance. In April, 2018, Aadhaar based e-authentication was made mandatory along with PAN for KYC by RBI pursuant to an amendment in the PMLA which literally left no option to the customers to use any other officially valid document like passport, driving license, etc. This exacerbated the privacy concerns around Aadhar and was seen by many as contrary to law and privacy tenets of choice and consent. Since the constitutionality of Aadhaar was already under challenge and the matter was already sub judice in the Supreme Court of India, the amendment to KYC guideline making Aadhar based KYC mandatory became subject to the outcome of the matter. The historical Aadhaar judgment by the Supreme Court was finally given on 26.09.2018 which again changed the way KYC was being undertaken.

What happened after the Aadhaar Judgement[2]?

The Hon'ble Supreme Court in the Aadhaar Judgment[3] held the use of the Aadhaar e-KYC/ authentication process by the body corporates and persons as unconstitutional and read down

[2] W.P. (Civil) No. 494/2012
[3] Ibid

Section 57 of the Aadhaar Act[4] virtually debarring corporate entities (including all Regulated Entities except a few) from using Aadhaar for authentication.

This was a huge blow and most entities were directed to stop using e- authentication and to close the authentication process in entirety[5]. Subsequently, Section 11A of the PMLA was amended[6] to allow banks to undertake Aadhaar based e-authentication and central government was permitted to allow certain Reporting Entities to undertake Aadhaar based e-authentication[7]

Offline KYC

Post Aadhaar Judgment, both Central Government and UIDAI were scampering to find alternatives to E-authentication to control the ramifications of the judgment to the fintech ecosystem. Aadhaar Paperless Offline e-KYC was already being used as an alternative to e-authentication and post the Aadhaar judgment it was extensively advertised and advocated as an alternative:

a) Offline XML Aadhaar - It is a secure sharable document that can be used by an Aadhaar Number holder for offline verification. An Aadhaar Number holder can generate an XML digitally signed by UIDAI by accessing UIDAI portal which will include the name of the holder, address, photo gender etc. Aadhaar Number holders are free to share this ZIP file along with the Password (Share Code) to Regulated Entities[8] as part of KYC. Thus, Regulated Entities can verify the demographic contents of the file and certify it to be authentic when doing offline verification.

b) QR Code: QR Code is present in all Aadhaar letters and the QR code is required to be scanned using the physical scanner in line with UIDAI Specifications using UIDAI's QR code reader application. The application will thereafter display the requisite details of Aadhaar Number holder once the relevant QR Code of Aadhaar is digitally verified by UIDAI at backend.

---

[4] **57.** Nothing contained in this Act shall prevent the use of Aadhaar number for establishing the identity of an individual for any purpose, whether by the State or any body corporate or person, pursuant to any law, for the time being in force, or any contract to this effect:

Provided that the use of Aadhaar number under this section shall be subject to the procedure and obligations under section 8 and Chapter VI.

[5] As per circular dated 23.10.2018, UIDAI based on opinion of Ld. Attorney General of India clarified that "Banks" are at liberty to use Aadhaar based e-authentication if provided voluntarily by the customer.

[6] W.e.f. 25.07.2019 vide Notification No. SO2649(E) dated 25.07.2019.

[7] Section 11A of the PMLA Ibid

[8] As per RBI Master Direction, 2016 on KYC (updated till 20th April, 2020 "Regulated Entities" (REs) means

a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'

b. All India Financial Institutions (AIFIs)

c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).

d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)

e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

Offline KYC has not been as successful as e-authentication. For example, UIDAI suggested using specialized hardware to scan QR codes which was an additional investment for majority of businesses. Also, the photo that is part of the QR code verification is usually a low-resolution photo and cannot be used at times for verification of the customer. Similarly, in case of XML there is no clarity on how to share the offline KYC XML with a service provider. While the file is password protected, the user needs to share the password with the service provider and the service provider may end up storing the data without the consent of the user.

What's new?

In January, 2020 the Master Direction - Know Your Customer (KYC) Direction, 2016 (now amended up to 20th April, 2020) **("New KYC Master Direction")** was amended to include two new ways of undertaking KYC pursuant to the amendment of Prevention of Money-laundering (Maintenance of Records) Rules, 2005[9]:

i. **Video KYC** (V-CIP)[10]

Under V-CIP, KYC is undertaken through Aadhaar e-kyc Authentication for banks and Aadhaar offline KYC for Regulated Entities other than banks and through live video interaction which is undertaken by an authorized official of the Regulated Entity. Business correspondents can facilitate the process only at the customer end and the official at the other end of V-CIP interaction should necessarily be a financial entity official. Basically, V-CIP involves verification of Aadhaar and PAN, matching of face on Aadhaar with face in video, which can also be through face recognition technology. Live location of the customer (Geotagging) is captured to ensure that customer is physically present in India. The Regulated Entities have to ensure that the process is seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. As the audiovisual interaction shall be triggered from the domain of the Regulated Entity itself, and not from third party service provider it also helps in reducing the chances of malpractice. RBI has also encouraged the use of AI however it is optional. Due to poor quality of photo in Aadhaar, RBI must seriously consider making atleast use of face recognition technology mandatory to rule out the possibility of fraudulent manipulations.

---

[9] Prevention of Money-laundering (Maintenance of Records) Third Amendment Rules, 2019 on 19th August, 2019

[10] "Video based Customer Identification Process (V-CIP)" is \ a method of customer identification by an official of the RE by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of the KYC Master Direction.

ii. **Digital KYC**

The Digital KYC is a cumbersome process when compared to Video KYC as the customer has to visit the authorized official of the Regulated Entity or vice versa. Other than that, the official has to take photo of the customer as well as the officially valid documents ("OVD") which has to be done in a particular manner as provided in the guidelines. Also, the system application of the Regulated Entity needs to be embedded with water-mark in readable form having Customer Application Form (CAF) number, GPS coordinates, authorized official's name, unique employee Code (assigned by Regulated Entities) and Date and time stamp on the captured live photograph of the customer. The authorized officer also has to provide a declaration about the capturing of the live photograph of customer and the original document. The live photograph of the authorized official is also captured in this authorized officer's declaration and OTP based verification undertaken. On successful verification, the CAF is then digitally signed by authorized officer of the Regulated Entity who takes a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scans and upload the same in system.

Other Developments

Recently two notifications have been issued by authorities which may forever change how KYC is undertaken:

a) On 22nd April, 2020 the Central Government has in terms of sub-section (1) of section 11A of the Prevention of Money-laundering Act, 2002[11] allowed certain Reporting Entities to

[11] 11A. Verification of identity by reporting entity
(1) Every reporting entity shall verify the identity of its clients and the beneficial owner, by--
(a) authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016) if the reporting entity is a banking company; or
(b) offline verification under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
(c) use of passport issued under section 4 of the Passports Act, 1967 (15 of 1967); or
(d) use of any other officially valid document or modes of identification as may be notified by the Central Government in this behalf:
Provided that the Central Government may, if satisfied that a reporting entity other than banking company, complies with such standards of privacy and security under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and it is necessary and expedient to do so, by notification, permit such entity to perform authentication under clause (a):
Provided further that no notification under the first proviso shall be issued without consultation with the Unique Identification Authority of India established under sub-section (1) of section 11 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016) and the appropriate regulator.
(2) If any reporting entity performs authentication under clause (a) of sub-section (1), to verify the identity of its client or the beneficial owner it shall make the other modes of identification under clauses (b), (c) and (d) of sub-section (1) also available to such client or the beneficial owner.
(3) The use of modes of identification under sub-section (1) shall be a voluntary choice of every client or beneficial owner who is sought to be identified and no client or beneficial owner shall be denied services for not having an Aadhaar number.
(4) If, for identification of a client or beneficial owner, authentication or offline verification under clause (a) or clause (b) of sub-section (1) is used, neither his core biometric information nor his Aadhaar number shall be stored.

undertake Aadhaar e-authentication like National Securities Depository Limited, Central Depository Services (India) Limited, Bombay Stock Exchange Limited etc., therefore, paving the way for use of Aadhaar based e-authentication for KYC process. This notification is pursuant to 9th May, 2019 notification of Department of Revenue Ministry of Finance which laid down the process for processing of application by Reporting Entities for use of Aadhaar authentication services under the power provided to central government to allow certain Reporting Entities to undertake Aadhaar based e-authentication and notification dated 5th November, 2019 of SEBI which allowed entities in the securities market to undertake Aadhar based authentication subject to certain terms and conditions.

b) SEBI has also come out with a circular on clarification on know your customer (KYC) process and use of technology for KYC[12](“**Online KYC Circular**”). To allow the ease of doing business in the securities markets it has allowed SEBI registered intermediaries (“**RI**”) to use e-signing as provided under the Information Technology Act, 2000 (“**IT Act**”) for signing of application forms and also provided the procedure for video in person verification for individuals. The RIs can provide this online KYC facility through their website or application or any other digital platform provided that it is adhering to all the security protocols as well as features like time stamping, geo location tagging of the investor to ensure the physical location of the investor is in India. Unlike the New RBI KYC Master Directions, Online KYC Circular provides that in case the investor uses Aadhaar e- authentication or offline Aadhaar for KYC verification or provides document through Digilocker[13] then there is no further requirement of in person verification/video in person verification (“VIPV”). It is only required in case the investor is relying on other OVDs.

Conclusion

1. V-CIP again moves the needle to undertaking KYC without the need for physical interaction. Video KYC is already being provided by some service providers and the Covid-19 pandemic is likely to be a catalyst for large scale shift to V-CIP. Unfortunately, Digital KYC makes the process of original seen and verified more complicated as it not only involves physical meeting between the authorized official and the customer but also adds on a lot of technical additions which could have been done away with. We are all for going digital but the idea is to move

(5) Nothing in this section shall prevent the Central Government from notifying additional safeguards on any reporting entity in respect of verification of the identity of its client or beneficial owner.

Explanation.-- The expressions "Aadhaar number" and "core biometric information" shall have the same meanings as are respectively assigned to them in clauses (a) and (j) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).]

[12] Circular dated 24.04.2020 – SEBI/HO/MIRSD/DOP/CIR/P/2020/73

[13] Digilocker is a facility provided pursuant to Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker facilities) Rules, 2016 which provides customers with the facility of uploading scans photos of OVD on a virtual lockers and also allows storage of electornic OVD issued by authorities and digitally signed by them.

away from direct face to face interaction. Unfortunately, Digital KYC irrespective of how grand it sounds does not tick all the boxes.

2. Another important point that seriously needs to be considered is sharing of information by Regulated Entities. In the New KYC Master Directions to verify the identity of customers, Regulated Entities can rely on customer due diligence done by a third party, subject to certain procedural conditions. However, the Regulated Entities do not usually upload KYC data in the Central KYC Records Registry because as even for uploading documents a certain amount has to be paid by the Regulated Entities. As observed and recommended in the Steering Committee Report, 2019 by Department of Economic Affairs, Ministry of Finance "The cost of on boarding a customer is an expensive proposition and, in this way, new banks are at a disadvantage. The Committee recommends that there should be no charge of uploading KYC data while every download can be priced up based on the user pays principle." Also, if a Regulated Entity has already undertaken KYC of a person then another Regulated Entity should not be required to repeat the procedure and it will save cost and time of all the parties. Therefore, it is imperative that necessary provisions are brought into place to ensure effective implementation of the sharing of KYC information.

3. This year we have taken some giant step towards making KYC process completely digital. Currently only SEBI has come out with online KYC and we can only hope that RBI will follow suit and implements it quickly. The reluctance so far in going digital has been the privacy issues and the inherent fear that digitally we will be unable to achieve what can be done manually. A classic example is digital KYC which while using technical advances goes back to finally the official verifying everything. To move forward, we have to look beyond our fears and understand that technology has grown in leaps and bounds in the last 5 years and with adequate system in place, we can look at making KYC completely digital in the right sense of the word. As Marie Claire said, "Nothing in life is to be feared, it is only to be understood. Now is the time to understand more, so that we may fear less."

- ***Ms. Akshaya Giridharan and Ms. Joyeeta Banerjee (Associate Partner)***
  with inputs from Ms. Shivi Rastogi (Partner)