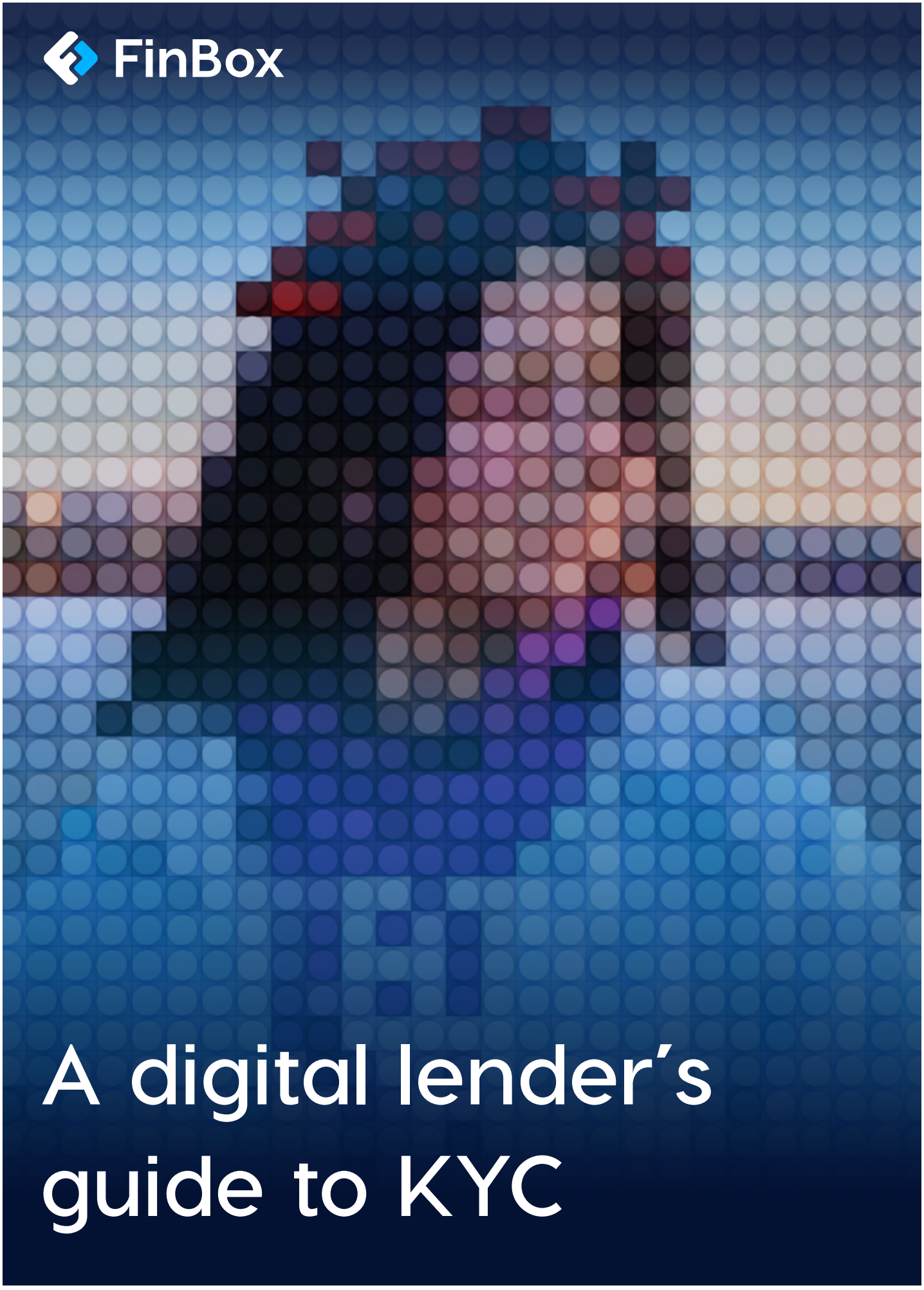
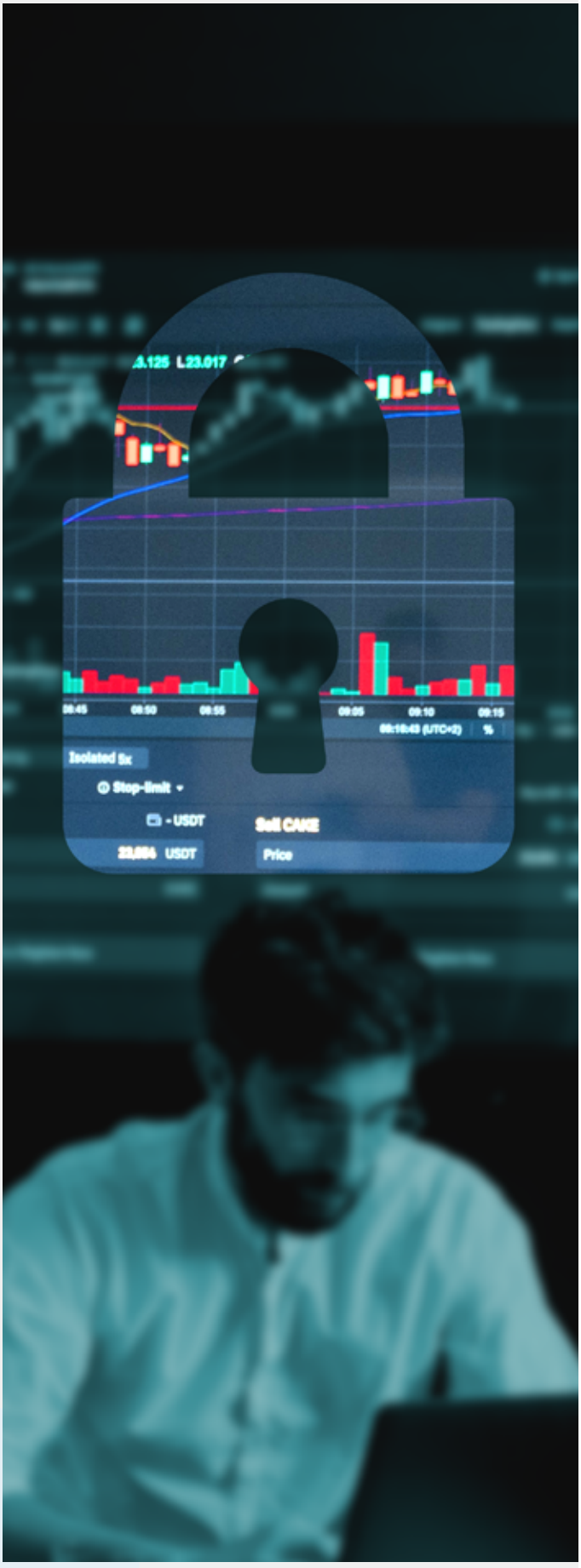
FinBox



A digital lender's guide to KYC

www.finbox.in

Table of Contents



Introduction

Financial crimes have long been the scourge of economies. A look at the history of these offenses shows that they have evolved alongside countries' financial systems. As a result, know-your-customer (KYC) guidelines by financial regulators of various countries came into force to check identity fraud, financial fraud, terror financing, money laundering and other financial crimes.

In the age of digitisation, lending and other financial services have been taken online. And along with these, financial crimes have also found a new playground. Fraudulent digital lending apps and unlawful harassment by seedy lenders has already drawn the attention of the RBI. The need for comprehensive KYC checks by digital lenders, in this context, is even more pronounced as it mitigates instances of financial crimes, including fraud, and establishes credibility.

Types of KYC

Lenders have left behind the early days of KYC when it was a tedious process involving cumbersome leg- and paperwork. After a series of notifications, regulations and judgments, the KYC landscape for digital lenders now looks extremely different from 2004, when the RBI first mandated it. Lenders can now conduct KYC using various methods.

Full and minimum KYC

However, the various methods of KYC can either result in 'full' KYC or 'minimum' KYC. The former allows customers to open accounts with lifetime validity and no cap on the transaction or account balance.

Minimum KYC, on the other hand, is only valid for 12 months and limits the account balance and transaction amount. Most importantly, minimum KYC is valid only if the information submitted by the customer is successfully audited.

Full KYC

1. *Physical KYC*

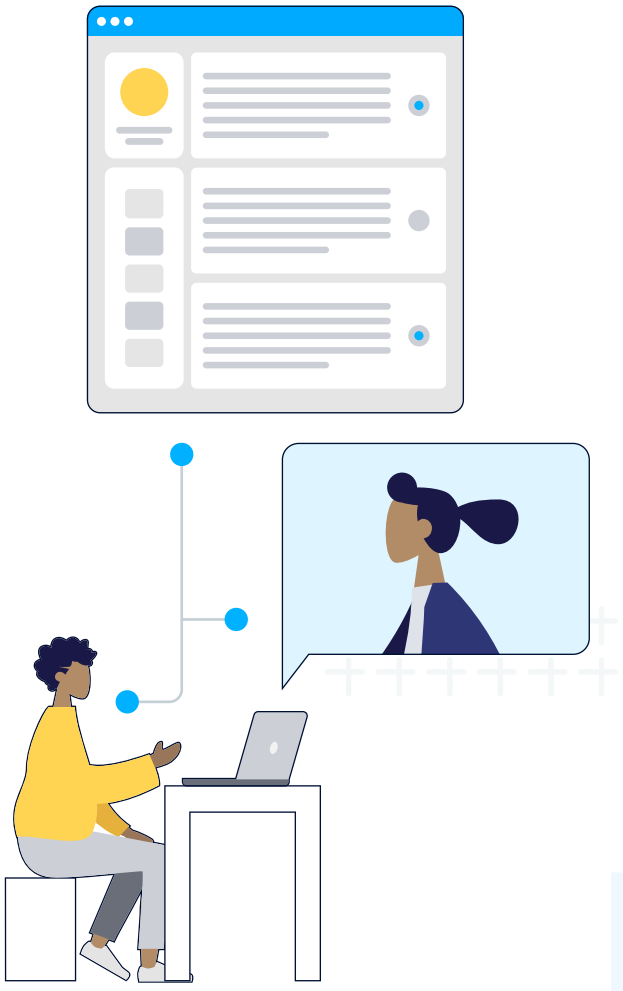
Physical KYC involves customers submitting self-attested copies of their identity and address proofs at the premises of the financial institution in question. While it was the norm prior to the introduction of digital KYC, now physical KYC is used for areas and demographics with poor digital education or penetration.

This approach to KYC involves a long turnaround time and is expensive since it involves manually authenticating and verifying documents. Costs of operation and storage add up to the overheads, making KYC costly, if not completely unviable for smaller digital lenders.

2. *Video KYC*

KYC can be carried out on a video call with an agent of the financial institution. Customers are required to submit their proofs of identity and address with a video recording. An agent of the financial institution then verifies and authenticates the video and the documents shared.

- **V-CIP:** Video-based Customer Identification Process (V-CIP) is a method of customer identification involving facial recognition by an official through seamless, secure and consent-based live audio-visual interaction. The customer is required to produce their OVDs during the interaction and the lender conducts an independent verification against the documents submitted.



Minimum KYC

Before we dive into the various methods of conducting minimum KYC, let's first understand what 'digital KYC' is. The RBI's Master Directions on KYC describe digital KYC something like this:

> *"Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the RE as per the provisions contained in the Act.*

This definition, effectively, suggests that digital KYC is any form of KYC that is **not physical or video KYC.** Lenders and FinTechs have interpreted this definition differently, allowing them to conduct e-KYC using various methods – all the while **ensuring the liveness of the customer.**

In the following graphic, we break down the RBI's directions around conducting digital KYC:

What constitutes Digital KYC?

- Shall be undertaken only through RE's authenticated application
- The RE must take a only live photographs compete with GPS coordinates and authorized official's details
- No printed or videographed photographs are allowed
- QR codes can be used to auto-populate the application form
- Once the form is filled, the customer must enter an OTP. this OTP will be treated as customer signature
- The RE's official shall provide a declaration about capturing the live photograph via OTP
- An RE official should match information provided by the customer with the picture and live photo with photo in the document

3. Aadhaar e-KYC

This is where the story of KYC in India gets complicated. Aadhaar e-KYC is a creature that has grown several heads, the complication arising out of the 2018 Aadhaar judgment. We'll get into the impact of the judgment on KYC regulation in a later section. For now, let's look at various types of Aadhaar e-KYC. Broadly, there are two categories within this KYC method – online and offline.

- **Online e-KYC:** Online e-KYC includes an OTP-based method and a biometric-based method. Under the first one, an OTP is sent to the mobile number of the customer. Biometric e-KYC involves matching the customer's retina or fingerprints with the UIDAI databases and seeking additional information from the authority.

- **Offline e-KYC:** After the Aadhaar judgment restricted FinTechs from seeking the Aadhaar numbers of users, the UIDAI introduced what have come to be known as 'offline' e-KYC methods. This approach shouldn't be confused with physical KYC.

  One way to do this is through uploading an XML file and share code of the user's Aadhaar details downloaded from the UIDAI website. Alternatively, FinTechs have been authorized to carry out Aadhaar e-KYC by allowing users to scan the QR codes on their Aadhaar cards and authenticate the details.

4. C-KYC

Central KYC requires the digital lender to download the customer's documents from the central KYC registry which is operated by the CERSAI.

Customers submit a signed C-KYC form along with proof of address and identity only once. This information is stored with the CERSAI's central databases. For every subsequent use, the customer need only authorize the entity to access this information for KYC.

The foremost criticism of C-KYC had been that the information submitted by the customer is not audited. In case this information is incorrect, it would result in a perpetual cycle of poor due diligence by all subsequent financial service providers seeking to do KYC.

Central KYC requires the digital lender to download the customer's documents from the central KYC registry which is operated by the CERSAI.

Customers submit a signed C-KYC form along with proof of address and identity only once. This information is stored with the CERSAI's central databases. For every subsequent use, the customer need only authorize the entity to access this information for KYC.

The foremost criticism of C-KYC had been that the information submitted by the customer is not audited. In case this information is incorrect, it would result in a perpetual cycle of poor due diligence by all subsequent financial service providers seeking to do KYC.

However, CERSAI announced in early 2022 that creditors have now been allowed to rectify omission or mis-statement of customer particulars in its databases. If such discrepancies are caught during an audit of KYC information, lenders can request the GOI to sanction the rectification. Moreover, it has now mandated that particulars collected during **all methods of KYC** now be reported to its databases, not just full KYC accounts.

Regulatory overview and entanglement with Aadhaar

The regulatory requirements of KYC have been intertwined with the regulatory history of Aadhaar. In 2018, the Supreme Court delivered its landmark Aadhaar judgment that barred private entities from seeking Aadhaar numbers from customers.

Subsequently, private entities have been allowed to conduct e-KYC through workarounds by the Ministry of Finance and UIDAI. Because of the ever-evolving regulatory oversight around Aadhaar, KYC regulation has also been hard to track.

Aadhaar judgment

The Aadhaar judgment of 2018 was significant for a number of reasons. For fintechs, however, the Supreme Court's partial quashing of section 57 Aadhaar Act was crucial. The Court struck down the phrase 'or any contract to this effect' in the main provision of section 57.

It now read:

> *"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~~".*

This effectively excluded fintechs from performing Aadhaar KYC, unless it was pursuant to any law. However, it could be interpreted that if an individual voluntarily chooses to use Aadhaar as proof of identity/residence, it would be considered valid.

RBI notification

In 2021, the RBI issued a circular allowing entities other than banks (NBFCs, payment system providers and payment system participants) to use Aadhaar authentication services through e-KYC provided by the UIDAI. This notification, read with the Finance Ministry's 2019 circular, allows non-banks to apply for a KYC User Agency (KUA) License or a sub-KUA license where 'necessary and expedient' to perform Aadhaar authentication.

What's allowed?

What is Aadhaar authentication?

Before we proceed, let's take a step back to understand a crucial concept - Aadhaar authentication. Here's how the Aadhaar Act defines it:

> *"Authentication" means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it;*
>
> *Section 2(pa) defines offline verification as the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations.*

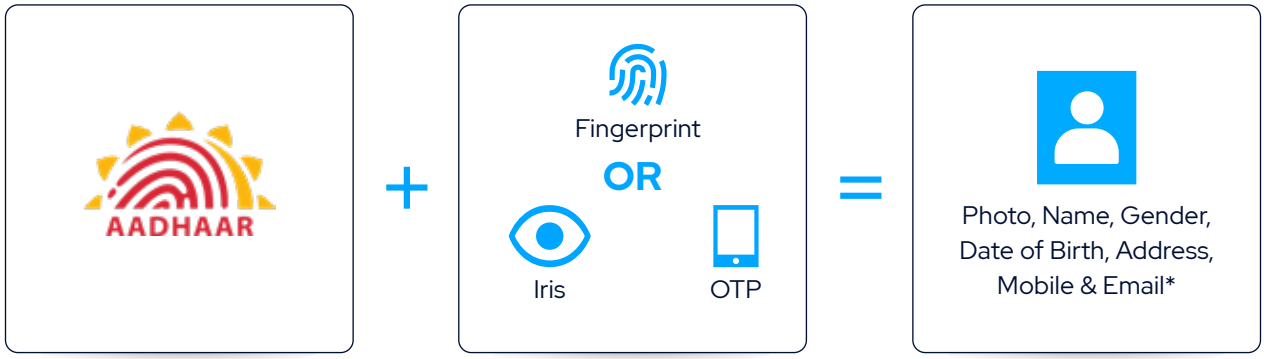
Aadhaar authentication can be done in three ways. It is important to note that all three methods require obtaining the customer's Aadhaar number :

1. **Demographic:** The demographic information of an Aadhaar number holder is matched against their demographic information held in the Central Identities Data Repository (CIDR).
2. **OTP-based:** The customer shares their Aadhaar number. Then, a one-time password (OTP) is sent on their registered mobile number to be entered into the journey. This is matched with the OTP sent to the UIDAI
3. **Biometric:** The customer's Aadhaar and biometric information are cross-checked with the biometric information stored with the CIDR.

However, since the Supreme Court restricted the non-banks from obtaining Aadhaar numbers, these methods of authentication elude fintech and TSPs.

How can these unregulated players and NBFCs conduct e-KYC?

- **Offline KYC:** Methods of **offline verification** already discussed above like XML and QR code-based authentication have been available for public use by the UIDAI. These **customer-initiated** methods of accessing Aadhaar details generate minimum customer details and are shared by customers **of their own volition, without the entity having to ask for the Aadhaar number.**
- **Online KYC:** Offline verification proves less resource intensive than biometric authentication, making it a favorable choice. However, following the RBI's notification, several fintechs and TSPs with KUA licenses have resumed the use of OTP-based KYC as well.



How to store and process Aadhaar data?

Aadhaar information, being highly sensitive, must be handled carefully by all players concerned. Here are some rules:

1. *Aadhaar Data Vault*

All registered entities and KUA/AUA/Sub-AUA license holders that store Aadhaar numbers must do so in a centralized Aadhaar Data Vault. This vault stores Aadhaar numbers in a masked manner through reference keys. It is a secure system inside the agency's infrastructure. It is accessible only on a need-to-know basis. It also aims to reduce the footprint of Aadhaar numbers within the organization's system.

2. *Scanned/hard copies*

Entities that store scanned and physical copies of Aadhaar, and do not store Aadhaar numbers separately, do not need an Aadhaar Data Vault. While the UIDAI doesn't specify the methods of storing hard copies, it states that these must be stored in a secure manner.

The agency states that scanned copies of Aadhaar must be stored in an encrypted form. Moreover, scanned copies with the card holder's photograph may be considered as biometric information. The processing and storage of these documents must be compliant with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 or the SPDI Rules – along with Aadhaar Act rules.

3. *Processing Aadhaar data*

Tech service providers and digital lenders (fintechs) are allowed to consume Aadhaar data only at the time of onboarding. Following this, they must purge this data. Unregulated entities are not allowed to store this information after KYC is complete. For the duration of the KYC process, they must store it in a masked manner.

The UIDAI has issued some other pointers for the treatment of Aadhaar data during processing:

- After collection, the Aadhaar number should not be displayed, published or posted publicly
- The collecting entity is responsible for confidentiality of the Aadhaar number and the database containing it
- Aadhaar numbers can be shared over the internet only after encryption

Despite these rules, the Sharing of Information Regulations are applicable only to the Aadhaar number. There is some lack of clarity around whether they are applicable to any document containing the Aadhaar number.

KYC checklist

1. *Officially valid documents including Aadhaar*

The RBI allows for the use of officially valid documents (OVDs) like

- Passport
- Voter ID
- PAN card
- Driver's license
- Proof of possession of Aadhaar
- NREGA job card signed by a state government official

With the introduction of Aadhaar e-KYC in 2013, this resource-intensive process became smoother, cheaper, and the norm. Even though the Aadhaar judgment threw a wrench in the works for digital lenders, eventually, they have been allowed to conduct 'offline e-KYC' – by way of QR codes and XML files.

2. *KUA license*

NBFCs, payment system providers, payment system participants and fintechs can apply for an Authentication User Agency (AUA) or e-KYC User Agency (KUA) license, where 'necessary and expedient', under Section 11A of the Prevention of Money Laundering Act, 2002.

As per the Aadhaar (Authentication) Regulations, 2016,

"Authentication User Agency" or "AUA" means a requesting entity that uses the Yes/ No authentication facility provided by the Authority;

"e-KYC User Agency" or "KUA" shall mean a requesting entity which, in addition to being an AUA, uses e-KYC authentication facility provided by the Authority

"e-KYC authentication facility" means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction;

3. *KUA license application*

These companies are required to submit an application to the appropriate regulator (in the case of lending, the RBI). The application is reviewed by the RBI to check if the applicant meets the security and IT-related requirements. The UIDAI checks for the applicant's compliance with its privacy and security standards.

The Finance Ministry's Department of Revenue has published a detailed process for such an application here. Here's a snapshot:

Application is submitted to the appropriate regulator. The RBI, in this case

↓

The application is reviewed by the RBI to check if it meets the components of Section 11A of the PMLA and security and IT-related requirements.

↓

The UIDAI checks for compliance with its privacy and security standards.

↓

The UIDAI sends a notification to the MoF's Department of Revenue

↓

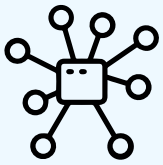
The MoF will notify as AUA or KUA

↓

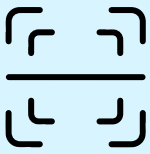
The UIDAI will authorize the licensee to use its authentication facility.

KYC cascade

There is no clear regulatory oversight regarding the use of the various KYC methods. In fact, players may or may not have the tech integrations to conduct each type of KYC. Assuming that a digital lender has the resources to conduct all types of KYC the following cascade is preferred:



C-KYC:
C-KYC is slowly becoming the most preferred method of KYC since it is convenient for both the customer and the entity conducting KYC.



O-KYC:
In case the customer does not have records with CERSAI, the next resort is XML or QR code-based KYC. This is second of C-KYC since it involves a degree of friction at the time of entering the CAPTCHA.

Online e-KYC/ video KYC:
OTP and biometric-based KYC is riddled with confusing regulatory scrutiny. Biometric and video KYC also tend to be resource-intensive, and therefore, not preferable.

How FinTechs can build a responsible KYC programme

Balance customer needs with risk management

KYC is often viewed as a necessary evil by digital lenders and customers alike. However, if done right, the KYC/onboarding process can help lenders establish a good relationship with their customers. The RBI allows for various methods to do KYC, including

- a comprehensive set of OVDs
- a provision for e-KYC
- KYC via video call
- CKYC

Digital lenders must build a scalable KYC programme that incorporates all these methods. Customers must be allowed to choose their favoured method of KYC depending on the documents available with them, and their access to mobile phones and internet connectivity.

However, in their bid to improve customer experience, lenders should not take away from their risk management imperatives.

- ***Routine audits***

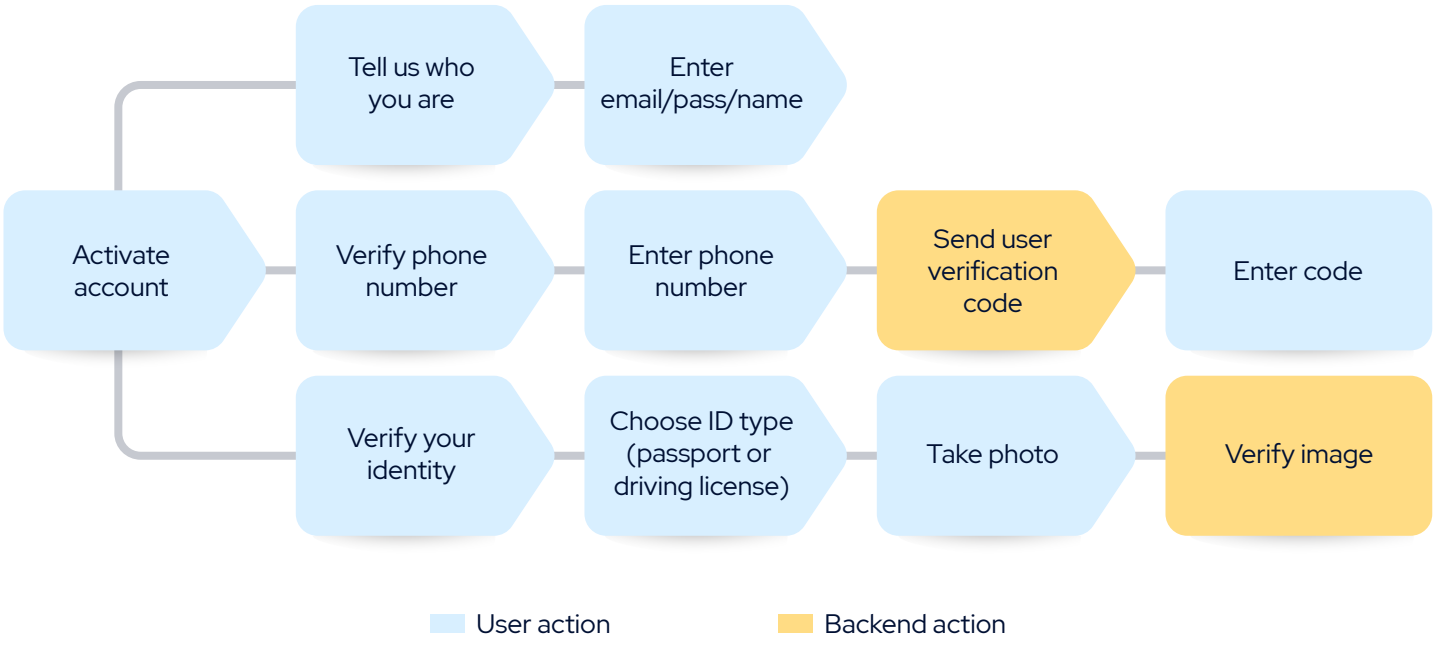
  They should carry out frequent audits in case of minimum KYC to ensure the validity of the process.

- ***CERSAI rectification***

  Earlier, just the presence of a customer's records with CERSAI was considered sufficient to successfully conduct KYC. With the provision of rectification, each digital lender should make it a point to request the correction of CERSAI information in case of mistakes and omissions.

Good UI/UX design

Even before the customer can apply for a loan, they are taken through a fairly complex KYC process. The challenge before a UI/UX designer is to create an experience that is easy to walk through while also ensuring it doesn't compromise on due diligence. This is what a typical KYC user journey looks like –

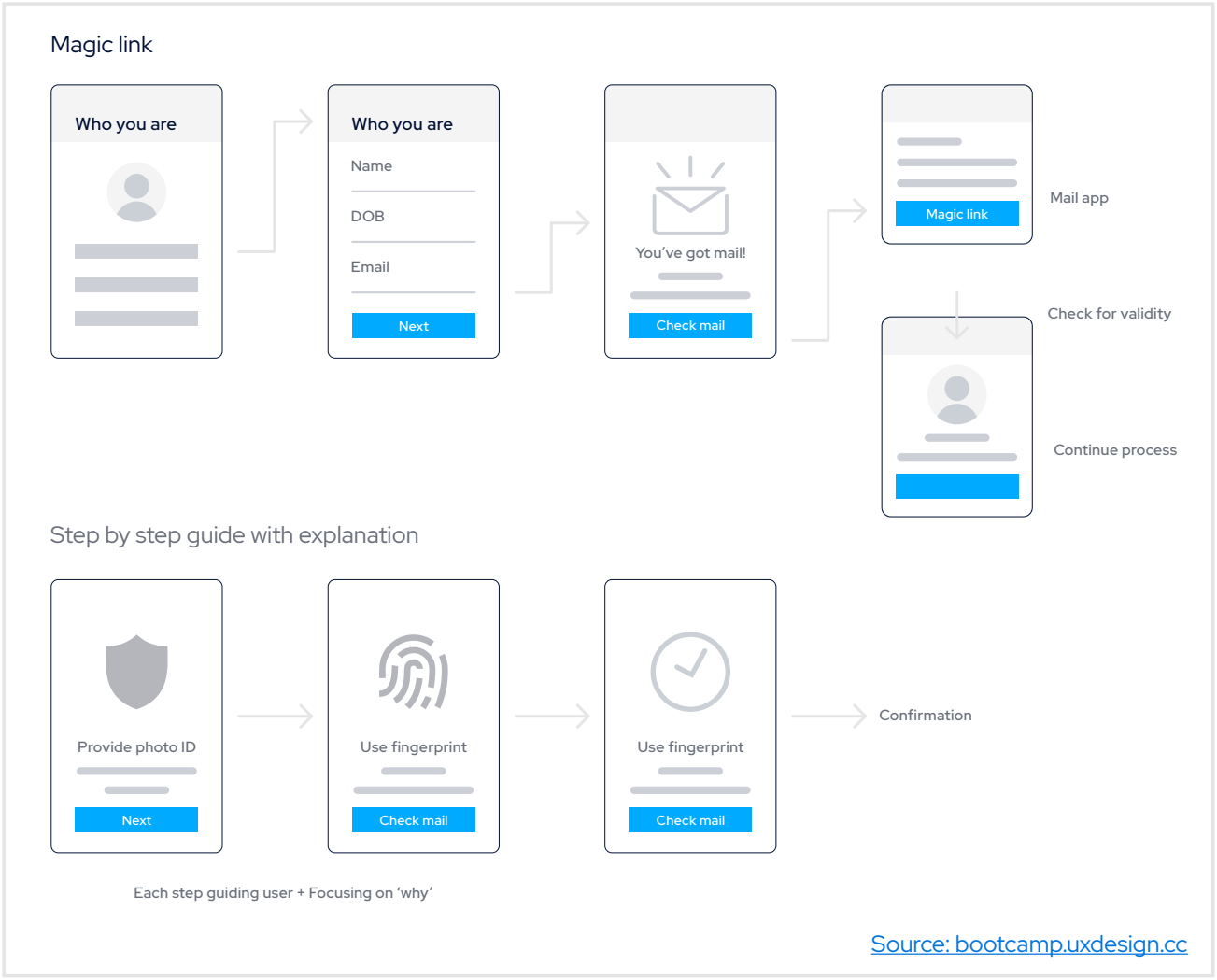


We list out some pointers that can help create compliance-first user journeys that also keep drop-offs at bay –

- Cleanly separate each step of the KYC journey. For instance, ask only for one piece of information at a time – email, phone number, OVD of choice, photo or verification code. Decluttering each screen helps reduce customer confusion and ensures smooth onboarding.

- When keeping the design clean and minimal, it may become difficult to incorporate all the complexities of KYC. It is imperative to present the logic behind the choice of the KYC process, the need for data sharing and storage, and the impact of selecting a certain method.

  Each screen should explain the 'why' behind the action required. In more complex cases, designers may create segues at critical points of the user journey and redirect customers to a more detailed explanation. Ideally, they must also incorporate chatbots or a customer service link where the user seeks further clarification.



Source: bootcamp.uxdesign.cc

- The use of graphics is integral to any minimalistic design. Use a combination of graphics and text that conveys the message as clearly as possible. The focus must be on artistic aspects like establishing a colour palette and iconography styles, along with clarity of message.

Automation

Automating certain KYC processes like case management, policy management and workflows can help increase capacity. Meanwhile, it can free up resources to focus on more value generating activities like risk assessment.

Data management

KYC requirements may be stringent, but lenders can focus on managing their data from various sources, internal and external, to create more advanced and dynamic KYC programs. For instance, they can manage and store initial KYC data to conduct periodic reviews seamlessly without asking for repetitive information.

Digital lenders must follow the UIDAI's directions on the collection, processing and storage of Aadhaar data in letter and spirit. For more information on these rules, refer to this document.

Periodic review

The RBI mandates that lenders conduct risk-based periodic updation every two years for high-risk customers, eight years for medium-risk customers and ten years for low-risk customers. The process of updation must be not only digitized, but personalized. Create user prompts for all possibilities during periodic review – no change in KYC information, address change, change in status from minors to majors, etc. Customers whose period review is due can be notified via push notifications, text messages or phone calls.

Appendix: Outsourcing of KYC

For FinTechs, it is essential to view regulations from an outsourcing perspective. FinTechs often function as technology providers to banks and NBFCs, which complicates their regulatory position. While there are no guidelines set in stone for outsourcing of KYC functions, the RBI has, time and again, released directions on outsourcing of financial and IT services by both banks and NBFCs.

The RBI is of the opinion that the REs are outsourcing critical IT services to tech providers extensively in order to improve efficiencies. However, it believes that these partnerships may expose these entities to financial, operational and reputational risks. This is why its guidelines place the onus to comply on the registered entities.

In this section, we lay out some of these directions and propose some best practices to be followed by FinTechs that can encourage compliance.

- ***REs must have a board-approved IT outsourcing policy***

  Outsourcing of services cannot diminish the obligations of the REs' or that of their senior management towards their customers. They are required to ensure that the service provider performs the activity with the same high standard of care as the RE would, were the activity not outsourced.

  What FinTechs can do: Incorporate the RBI's directives, suggestions and guidelines into their own company policies and ensure teams adhere to these practices, officially and unofficially.

- ***REs must have a robust grievance redressal mechanism***

  The RBI's Draft Master Direction on Outsourcing of IT Services states that the entity outsourcing the service must create a grievance redressal mechanism that should not be compromised, even on account of outsourcing. The responsibility for redressal of customers' grievances related to outsourced services would rest with the RE.

  What FinTechs can do: Work closely with their licenced lending partners to create a joint, if not common, grievance redressal mechanism for the duration of their partnership. Allowing the RE an inlet into the FinTech's own grievance redressal mechanism will eliminate unnecessary points of contact and lead to quicker solutions.

- ***Risk management framework***

  As per the draft, a risk management framework for the outsourcing of IT services should comprehensively deal with the processes and responsibilities for the identification, measurement, mitigation/ management and reporting of risks associated with outsourcing.

  Entities regulated by the RBI should also require their service providers to develop and establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

  What FinTechs can do: Apart from ensuring the robustness of their own risk management frameworks, FinTechs can rely on the expertise of their licensed partners to fine-tune their frameworks based on their regulatory requirements.

- ***Decision-making functions of determining KYC compliance norms can't be outsourced***

  Regulated entities cannot outsource their own decision making when it comes to compliance with KYC norms. The decision on KYC compliance lies squarely with the lender, without external intervention. The role of FinTechs in this respect is diminished.

Author's Bio

Rajat Deshpande,

Co-Founder and CEO, FinBox

Rajat is a Fintech specialist and a startup enthusiast who started FinBox along with his Co-Founders with a mission to lay out digital infrastructure for alternate finance solutions. Under his leadership, FinBox has built multiple products in the Embedded Finance and Big Data credit analytics spaces. FinBox has enabled over 16 million lending decisions in India and SE Asia. In his prior stints, Rajat was associated with the global consulting firm ZS, Citigroup and GoPigeon Logistics as Head of product.

He holds a Dual (BTech+MTech) degree in Mechanical Engineering from IIT, Bombay.

LinkedIn profile

Anant Deshpande,

Co-Founder, FinBox

Anant is a co-founder of FinBox. At FinBox, Anant leads lending and builds credit origination systems powered by alternate data and traditional data.

In his earlier role at Home Credit, he drove Big Data based loan underwriting of a $2B consumer loan portfolio. Anant has previously been associated with global consulting firm ZS Associates and TransOrg Analytics where he owned P&L and productised analytical consulting. He is a regular marathoner and holds a B.Tech in Chemical Engineering from Nagpur University.

LinkedIn profile

Chitwan Kaur,

Content Specialist, FinBox

Chitwan is a content specialist at FinBox involved in building thought leadership and responsible for our social media. Prior to FinBox, she worked at CNN-News18 where she manned the politics and breaking digital news desks. She holds a degree in English Literature from Delhi University and a post-graduate diploma in journalism from the Asian College of Journalism.

LinkedIn profile