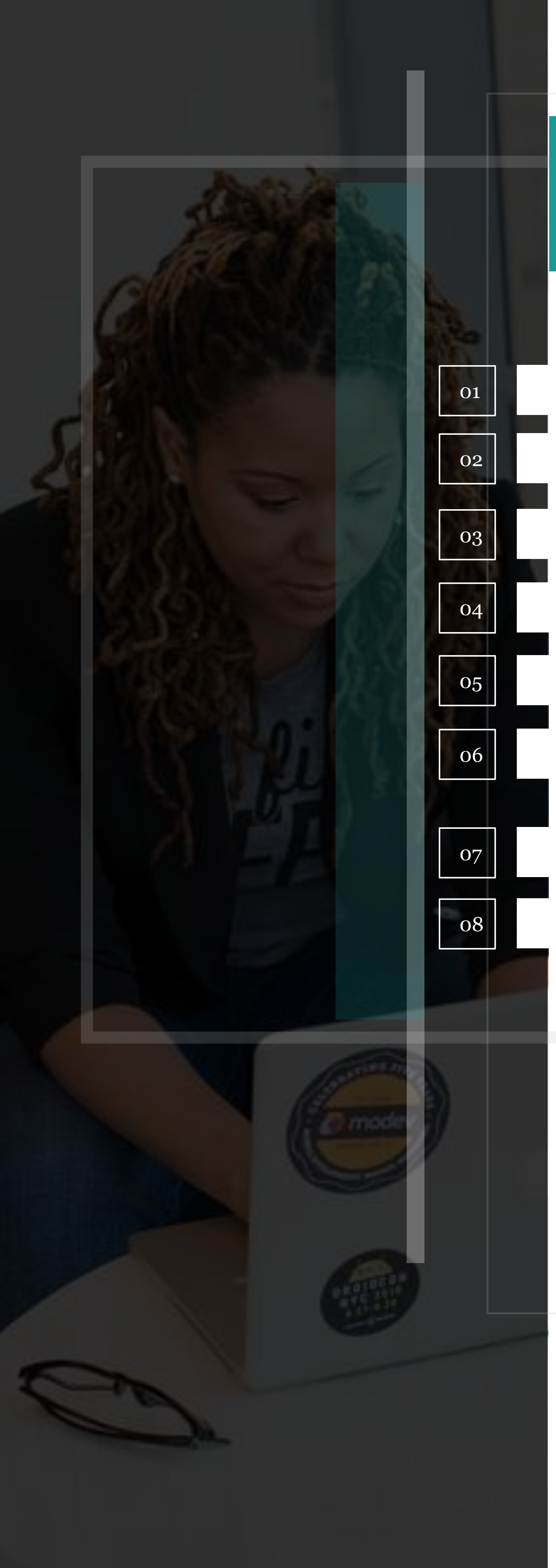
# Customer onboarding and engagement:

A white paper on a modern approach to KYC for financials services in a digital world



# Abbreviations

| | | |
|---|---|---|
| 01 | BVN | Bank Verification Number |
| 02 | CDD | Customer Due Diligence |
| 03 | GDPR | General Data Protection Regulation |
| 04 | KYC | Know Your Customer |
| 05 | NDPR | Nigeria Data Protection Regulation |
| 06 | NIMC | National Identity Management Commission |
| 07 | SMS | Short Messaging Service |
| 08 | USSD | Unstructured Supplementary Service Data |

# 1. Introduction

> The three main drivers for KYC are money laundering, tax evasion, and the financing of terrorism."

Knowing the identity of your counterparty has been fundamental to doing business for as long as time itself. With the nature of interactions and transactions in banking and financial services, it becomes imperative to know more than just the identity. However, determining whom you can and should do business with has a significant cost, time, and resource implications for financial institutions. According to a recent **KYC compliance survey**, the average annual spend on global KYC is reported as **US$48 million,** and onboarding times remain lengthy, with banks reporting an average time of **30 days.**

Relying on a patchwork of resources may leave potential gaps in coverage where **bad players can hide** while putting your revenue and reputation at risk from regulators.

Know Your Customer, sometimes referred to as Customer Due Diligence, is meant to verify the identity of customers and assess their suitability to be a customer. While customers universally consider KYC to be burdensome, it is crucial for businesses.

Throughout this document, Know Your Customer and/or Customer Due Diligence will be referred to as KYC.

The three main drivers for KYC are money laundering, tax evasion, and the financing of terrorism. Due to these, KYC policies have now evolved into an important tool to combat illegal transactions in national and international finance arenas. KYC allows businesses to protect themselves by ensuring that they are conducting business legally and with legitimate entities. Furthermore, it protects individuals who might otherwise be harmed by financial crime.

## How customers have evolved in the digital world

Due to the advent of digital technologies, customers have evolved from interacting with businesses on only traditional channels to digital channels. Customers are now used to convenience in onboarding and transacting with service providers. This change in customer behavior has led to KYC also evolving.

KYC has evolved from physical verification of customers by reviewing documentary pieces of evidence to the validation of customers across digital platforms using real-life images, scanned or uploaded identity documents, etc. API services are integrated to validate images, liveliness, and credentials provided by the customer, etc.

## How KYC is currently done.

In practice, KYC is conducted by obtaining and reviewing the customer's name, photograph on an official document that confirms their identity, residential address, and date of birth. The varying requirements for KYC for customers are closely related to the risk level of such customers and the nature of products or services offered by the business.

**Levels considered when carrying out CDD/KYC:**

**Simplified customer due diligence**

This can be applied when a risk assessment has shown a negligible or low risk of money laundering/tax evasion/terrorism financing. The only requirement for this level is to identify the customer without a need to verify the customer's identity.

**Standard customer due to diligence**

This involves identifying the customer based on a reliable, independent source or multiple sources. The purpose and intended nature of the business relationship or transaction must be assessed, and further information obtained where appropriate.

**Enhanced customer due diligence**

Enhanced KYC/CDD must be applied when the risk of money laundering/tax evasion/terrorism financing is high. An example is if the person in question is a politically exposed individual or a business entity involved in high-risk business activity. Enhanced due diligence measures can include:

- Additional identification information from the customer
- Information on the source of funds or source of wealth
- The intended nature of the business relationship
- The purpose of the transaction
- Subjecting the customer to additional ongoing monitoring procedures
- Ultimate Beneficial Owner

## Why customer engagement must change

Having recognized that access to basic banking and other financial services is necessary for achieving the Central Bank of Nigeria (CBN) policy on financial inclusion, there is a need to revisit the measures through which customers would usually be engaged, which has up until date, been mostly through physical channels.

More so, the pandemic in recent times has emphasized the need to digitize customer engagement, with virtual being the new norm. This has now placed more demands on the need for digital customer onboarding and provision of support. This would indeed require an extension of customer validation and onboarding to digital channels such as chat, phone, video conferencing, etc.

# 2. A Primer on KYC

> The **money** from the criminal activity is considered 'dirty,' and the process "launders" it to make it look clean.”

## What's KYC

Know Your Customer and sometimes referred to as Customer Due Diligence is the process of identifying **customers** and checking whom they say they are. It involves verifying the identity of customers and assessing their suitability to be a customer.

KYC regulations have far-reaching implications for consumers and are increasingly becoming critical issues for just about any institution that has to interact with money (so, just about every business). So, while banks are required to comply with KYC to limit fraud, they also pass down KYC requirements to individuals and organizations they do business with.

## Reasons for KYC

Before a Financial Service Provider can onboard a new customer, the truthfulness and accuracy of the customer's documentation must be ascertained. This helps the financial service provider prevent fraud and money-laundering while creating the opportunity to assess the customer's credit risk accurately. The three main drivers for KYC are:

### Money laundering

Money laundering is a common technique used by financial criminals and others to hide illegalgains. It is the illegal process of making large amounts of **money** generated by criminal activity, such as drug trafficking or terrorist funding, appear to have come from a legitimate source. The **money** from the criminal activity is considered 'dirty,' and the process "launders" it to make it look clean. A real-life example would be the case of **Pablo Escobar. His escapades contributed to the development and enforcement of the Money Laundering Control Act and The Anti-Drug Abuse Act**

Pablo Escobar was a prominent figure in the drug smuggling movement, smuggling 70-80 tons of cocaine to the US on a monthly basis at the peak of his career. This led to billions of dollars leaving the US, which had an impact on economic growth.

Nigeria has, in recent times, been labeled as one of the most corrupt countries in the world, with money laundering being one of the most prominent international criminal activities being perpetrated. Efforts by the Government through the activities of the Economic and Financial Crimes Commission (EFCC) and other agencies have not yielded many results. In Nigeria, all financial institutions are, by law, mandated to comply with the guidelines of the Money Laundering (Prohibition) Act 2011 and Money Laundering (Prohibition) (Amendment) Act 2012.

### Tax Evasion

Tax evasion is an illegal activity in which a person or entity deliberately avoids paying a tax obligation. Those caught evading taxes are generally subject to criminal charges and substantial penalties.

Tax evasion and avoidance reduce government revenues. This has a significant detrimental effect on the provision of infrastructure, public services, and public utilities. Multi-national companies (MNCs) in the oil, gas, and manufacturing sectors have used various tax avoidance schemes, including setting up off-shore intermediary companies, claiming recharges, royalties, or technical fees, and under-reporting of profit, to avoid paying tax in Nigeria.

### Terrorism Financing

Terrorism financing is the provision of funds or providing financial support to terrorists or non-state actors. Most countries have developed and implemented measures to counter-terrorism financing as part of their money-laundering laws.

The United States of America's Justice Department in 2014 placed some Nigerian banks under investigation in the wake of growing terrorism in the country. Specifically, the banks were investigated to establish their links, if any, with funding various terror cells across the continent. The development was a sequel to BNP Paribas' guilty plea and agreement to pay nearly $9 billion for violating U.S. sanctions, which triggered fresh enthusiasm in the U.S. Justice Department to also extend its investigations to Africa, especially among big banks on the continent with strong international links. Two other major French banks- Credit Agricole and Societe Generale, Germany's Deutsche Bank AG, and Citigroup Inc's Banamex unit in Mexico were among those investigated for money laundering or sanctions violations.

## KYC Tiering

In 2013, the Central Bank of Nigeria introduced a tiering structure that involves flexible account opening requirements to address vulnerable account holders who are financially excluded due to the onerous burden of providing documentation to prove their identity and income.

This Tiering policy is anchored on the risk level as well as the information provided by the customer. The process helps organizations to understand the customers' situation from their financial data and know that the services that should be provided to them.

## History of KYC

KYC laws were introduced in 2001 as part of the USA Patriot Act, which was passed 45 days after 9/11 to provide a variety of means to curb terrorist behavior.

The section of the Act that pertained specifically to financial transactions added requirements and enforcement policies to the USA Bank Secrecy Act of 1970 that had thus far regulated banks and other institutions. These changes had been in the works for years before 9/11, but the terrorist attacks finally provided the political momentum needed to enact them. Thus, 'Title III' of the Patriot Act requires that financial institutions deliver on two requirements to comply with the stricter KYC: the Customer Identification Program (CIP) and Customer Due Diligence (CDD).

It all started with the first recorded incident of Tax evasion, which is said to have happened in China approximately 4000 years ago. Merchants would hide their wealth from rulers in order to avoid it being taken from them. In modern terms, we call it tax evasion. However, and perhaps somewhat surprisingly, the foundation of modern KYC laws was not laid until the 1950s.

KYC has undergone a metamorphosis and should no longer be viewed as simply a cost that organizations have to bear. Robust KYC is crucial to identifying risk as early as possible, but more importantly, it has become a strategic tool that can deliver a competitive advantage. The right technology can free compliance professionals from performing tasks that are often low value, repetitive, or time-consuming so that they can concentrate on higher value-add tasks. By harnessing the power of emerging technologies, organizations can ensure that their KYC procedures can lower costs, streamline operations and, ultimately, provide a better client experience.

## Tools for KYC

Different tools are used to verify a Customer's identity. Depending on what needs to be validated, different information sets are requested from a customer who needs to be reviewed and confirmed. The depths to which customer information needs to be validated are centralized based on whether a client or customer fits an organization's established risk profile before entering into a business relationship with the customer.. This ensures that identity thefts and any potential forgeries can be detected early on. Here are a few of these requests and how in today's world, the data provided by customers can be validated.

1. Biodata, this includes name, age, and sex. These are verified with:
    a. Birth certificate
    b. Government-issued identification like (International Passport, Driver's license, Govt ID or Passport, BVN, NIMC, etc.)
    c. Bank Verification Number (BVN)

2. Proof of Address
    a. Certified bank statement,
    b. A recent utility bill, usually not more than three months old
    c. Tax bill
    d. Postal-delivered verification code

3. Proof of Nature of Business
    a. Business Registration Document
    b. Licenses
    c. Memorandum and Article of Association

4. Disclose Source of Funds
    a. Recent payslip from employer
    b. Sale contract of a personal asset (a house, a car, a company, etc.)
    c. Certified bank statement (savings account extract, salary deposits, etc.)
    d. Heritage/gift (copy of the will, notarized letter, etc.)
    e. Loan agreements
    f. Other supporting documents (a letter signed by a lawyer or a Notary Public, etc.)

5. Corporate Governance
    a. Internal Policies

# 3. Challenges with KYC in the digital era

> Some countries, such as Nigeria, do not have a functional central identity registry."

To cope with the regulatory changes in data security and compliance, like NDPR, the need for automation is high. Increased investment in technology is required to drive automatic data onboarding, management of sensitive data, and support of data enrichment processes. Some of the current state challenges experienced with KYC include:

### Lack of Consistency

A common challenge faced by banks and Fintechs is a lack of standardization in methods for collecting information from customers. The documents requested from customers differ across banks and Fintechs.

### Limited Scalability

The current methods used for KYC are not scalable, especially when customers are in remote areas, abroad, or when a pandemic occurs, which makes physical interactions impossible or downright dangerous. Physical KYC validation can no longer suffice in these times.

### High Cost

The cost involved in KYC continues to rise. Due to this remarkable significance of KYC compliance, the identity verification industry is gaining hype, and it is expected to grow at a growth rate of 16% during the period of 2019 to 2024. The demand for KYC screening solutions is also increasing as it shares the compliance burden of the businesses. These solutions deliver highly accurate KYC screening results within seconds. So, businesses prefer these cost-effective KYC solutions instead of hefty manual verification solutions.

This rising cost of conducting KYC is prompting banks and Fintechs to consider cost-benefit analysis before onboarding a customer for a particular product or service. To cut costs, a financial institution performing KYC might decide not to onboard a customer if the cost for conducting KYC much outweighs the potential revenue from providing products or services to that customer.

## Where traditional KYC fail

### Identity verification

Some countries, such as Nigeria, do not have a functional central identity registry. Even where they do, the lack of modern technology makes accessing the identity registry difficult, costly, and time-consuming. Therefore, forgery is inevitable as there is no single source of truth for an individual's detail. This is one of the major reasons online transactions and other financial engagements are distrusted in emerging countries.

### Address verification

In recent times there has been an evolution in real estate where individuals can now rent spaces for as short as one week to a month, and this is becoming the new norm, especially for traveling business people and young professionals. Consequently, the proof of an address using a recent utility would no longer be relevant as a means of KYC, as this is pretty much volatile.

Likewise, for businesses, a lot can be done these days remotely and for those who still need physical locations because of clientele or regulatory reasons use remote workspaces, virtual offices, and the likes to account for these. This, therefore, invalidates the need to conduct address verification exercises, as different businesses can share or have shared the same desk space.

### Job and wealth profiles

Career growth and personal development have created limits to the validity of historical KYC done because as people age and develop themselves, their financial profile changes, which thus invalidates an old income profile.

## The risks that await traditional KYC

The traditional method of conducting KYC needs to change. This need for change is driven by the following:

- Customer expectations have changed
- Transaction profiles have changed
- Threats and forgeries are evolving

**Risks of pandemics have not abated**

# 4. Why bankers and finance experts are scared of introducing better KYC

> "It has been noticed so far that the KYC regime in Nigeria, especially has remained static."

**Poor understanding of the first principles of KYC**

The stringent regulatory environment establishes KYC as a mandatory and crucial procedure for financial institutions as well as non-financial institutions. KYC minimizes the risk of fraud by identifying suspicious elements earlier on in the customer-business relationship. For the purposes of a KYC policy, a customer/user may be defined as:

- a person or entity that maintains an account or has a business relationship with the reporting entity;
- one on whose behalf the account is maintained (i.e., the beneficial owner);
- beneficiaries of transactions conducted by professional intermediaries such as stockbrokers, Chartered Accountants, or solicitors, as permitted under the law; or
- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, for example, a wire transfer or issue of a high-value demand draft as a single transaction.

Today, KYC principles apply to banks, other financial institutions, and online businesses. KYC policies are usually framed, incorporating the following four key elements:

- Customer acceptance policy;
- Customer identification procedures;
- Monitoring of transactions; and
- Risk management.

**Lack of process engineering experience**

It has been noticed so far that the KYC regime in Nigeria, especially has remained static. As things evolve, there is a persistent need for entities to reengineer the KYC and onboarding process and look out for better ways to handle these changes.

**Limited technology solutions**

Most banks and banking applications don't have the necessary tools or features to virtually onboard or support customers without physically engaging them.

# 5. A new approach to KYC

> Verifying the income of individuals should go beyond just the review of employment contracts.

### How technology solves KYC issues

KYC is an important part of any business. In order to provide financial services online, companies need to have methods for remote identification in order to be aligned with KYC standards.

### Issues with traditional KYC and how digital approaches solve them

**Identity**

Identity in Nigeria today has been reconciled with Bank verification Number. With the BVN validation endpoint, customers no longer need to provide their names and other related information as this is fetched from the response retrieved from a successful validation.
The approach for validating customer identity can vary from platform to platform. Some examples are:

- Using DOB to complete the validation
- Using OTP to complete the validation

**Address verification**

Verifying the address of businesses and individuals is a critical compliance process for background checks, pre-employment screening, or tenancy vetting. Solutions like VerifyMe, SmileID, and of recent, NIPOST, in partnership with YouVerify, have provided means to verifying an individual/entity's location and provided address.

**Income verification**

Verifying the income of customers using traditional methods can be ineffective, especially as individuals and businesses hardly have the same income profile for a long period of time. Verifying the income of individuals should go beyond just the review of employment contracts. Digital technology can be leveraged such that the customer's statement can be automatically reviewed to ascertain the customer's income profile in seconds. This also would be effective for individuals who have multiple sources of income.

# 6. A proposed approach for KYC tiering

> We are proposing an alternative approach to KYC, and customer-risk tiering…"

## Introduction

Existing KYC tiering still works, but it has an element of being a means to an end. Emphasis is currently placed more on verifying the details provided when, to some extent, not all Tier levels, which is supposed to represent the risk level of a customer, should insist on verification.

We are proposing an alternative approach to KYC, and customer-risk tiering that takes into cognizance the evolved digital profile of customers, companies, and means of doing business. The proposed KYC would be applicable to individuals and non-individual entities (companies, non-profit, registered business names, partnerships, etc.) and would be largely dependent on risk levels.

In this proposed tiering approach highlighted in the table 1, items with 'required' mean the details would be collected from the individual or entity but verifying these details would not be necessary. There would be a concept of lifetime limit, which means that when an individual or entity reaches said limit, they would be required to move up to the next tier.

# KYC Tier for Individual Customers

For individuals, the proposed tier would be based on CBN's regulation

Table 1

| Requirement | Tier 0 | Tier 1 | Tier 2 | Tier 3 |
|---|---|---|---|---|
| Image liveness detection | | **REQUIRED** | **VERIFIED** | **VERIFIED** |
| Name | **REQUIRED** | **REQUIRED** | **VERIFIED** | **VERIFIED** |
| Email | **REQUIRED** | **REQUIRED** | **VERIFIED** | **VERIFIED** |
| Phone Number | | **VERIFIED** | **VERIFIED** | **VERIFIED** |
| date of birth | | **REQUIRED** | **VERIFIED** | **VERIFIED** |
| Address | | **REQUIRED** | **REQUIRED** | **VERIFIED** |
| Citizenship | | **REQUIRED** | **VERIFIED** | **VERIFIED** |
| Previous Names | | | **REQUIRED** | **VERIFIED** |
| Income | | | **REQUIRED** | **VERIFIED** |
| Daily Deposit Limit | | | | |
| Daily Withdrawal Limit | | | | |
| Lifetime Deposit Limit | | | | |
| Lifetime Withdrawal Limit | | | | |

## KYC Tiers for Non-Individual Customers

**Corporate KYC** is a process of validating the identity of business executives. This is a prerequisite to authenticating **corporate** accounts.

Table 2

| Requirement | Tier 0 | Tier 1 | Tier 2 | Tier 3 |
|---|---|---|---|---|
| Directors | | | **REQUIRED** | **VERIFIED** |
| Company Name | **REQUIRED** | **REQUIRED** | **VERIFIED** | **VERIFIED** |
| Business Phone Number | **REQUIRED** | **VERIFIED** | **VERIFIED** | **VERIFIED** |
| Business Email | **VERIFIED** | **VERIFIED** | **VERIFIED** | **VERIFIED** |
| Business Address | | **REQUIRED** | **VERIFIED** | **VERIFIED** |
| Director's Address | | | **REQUIRED** | **VERIFIED** |
| Nature of Business | | | **REQUIRED** | **VERIFIED** |
| Source Of Revenue | | | **REQUIRED** | **VERIFIED** |
| Source of Capital | | | **REQUIRED** | **VERIFIED** |
| Tax Compliance | | **REQUIRED** | **REQUIRED** | **VERIFIED** |
| Corporate Governance | | | | **VERIFIED** |
| Daily Deposit Limit | | | | |
| Daily Withdrawal Limit | | | | |
| Lifetime Deposit Limit | | | | |
| Lifetime Withdrawal Limit | | | | |

# 7. A summarized approach to digital onboarding and customer engagement

> Verifying the income of individuals should go beyond just the review of employment contracts.

## Assumptions

In order to create guidelines for digital onboarding and customer engagement journeys, certain assumptions have to be made. These include:

1. Key references made to BVN assume that onboarding and customer engagement journeys exist only within Nigerian financial jurisdictions. However, these journeys can be easily modified to fit into any country where an onboarding process would need to be completed digitally
2. The process of verifying customer details does not need to be prescribed, as different channels or jurisdictions may have different methods of verification
3. Where customer data are collected but not verified, it is expected that client and server-side checks would be done to ensure syntactical correctness
4. Verification should involve review and inspection in order to establish that provided evidence or information meets KYC requirements.
5. Validation should involve proving the accuracy of the presented evidence or information.

## Digital Onboarding for Individuals

The following is a summarized digital onboarding journey for an individual who would be requesting a service.

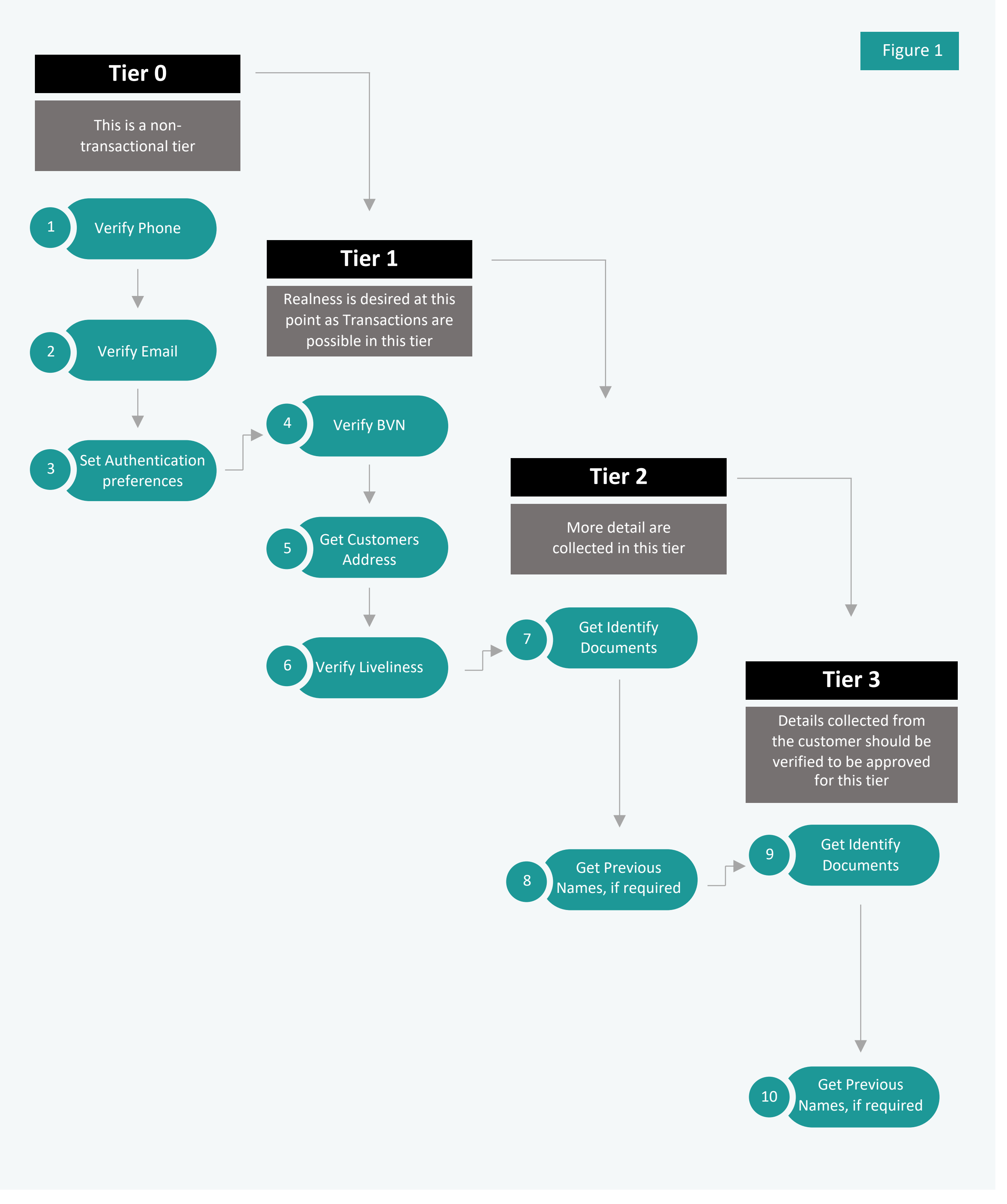


Figure 1
Tier 0
This is a non-transactional tier
1 Verify Phone
2 Verify Email
3 Set Authentication preferences
Tier 1
Realness is desired at this point as Transactions are possible in this tier
4 Verify BVN
5 Get Customers Address
6 Verify Liveliness
Tier 2
More detail are collected in this tier
7 Get Identify Documents
8 Get Previous Names, if required
Tier 3
Details collected from the customer should be verified to be approved for this tier
9 Get Identify Documents
10 Get Previous Names, if required

## Understanding the Onboarding Customer Journey for an Individual

1. Verify phone number: Customer inputs a phone number which can be verified by
    a. Sending an OTP to the customer to complete the onboarding process
    b. Initiating a voice call and OTP is given to the customer on the call to complete the onboarding process

2. Verify Email: Customer inputs an email address which can be verified by
    a. Sending an OTP to the customer to complete the onboarding process
    b. Sending an embedded link that redirects the customer to the next phase of the onboarding process.

3. Set Authentication Preferences: Different authentications are available today, and for most financial applications, multi-factor authentication is advised. **Multi-factor authentication** (MFA) is a security system that requires more than one method of **authentication** from independent categories of credentials to verify the customer's identity for a login or other transaction. There are generally three recognized types of authentication factors:
    **a. Type 1 – Something You Know –** includes passwords, PINs, combinations, code words, or secret handshakes. Anything that you can remember and then type, say, do, perform, or otherwise recall when needed falls into this category.
    **b. Type 2 – Something You Have –** includes all items that are physical objects, such as keys, smartphones, smart cards, USB drives, and token devices. (A token device produces a time-based PIN or can compute a response from a challenge number issued by the server.).
    **c. Type 3 – Something You Are –** includes any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification.

4. Verify BVN/National Identity Number: In terms of National Identity Number in Nigeria today, the tools available are BVN and NIMC. BVN is the most widely accepted as it is directly linked to the individual's financial identity. Not only does this Identification number serve as a KYC verification tool, but also a means to streamline the onboarding process.

5. Get Customer's Address: Here, the address of the individual is required in this stage but not mandatory to verify.

6. Verify Liveliness: Being a transactional Tier with requirements for elevated security and Customer experience, liveliness needs to be verified. There are two ways to check liveness:
    **a. Passive Liveness Check** – Using artificial intelligence to distinguish a real face from an image even without Customer interaction.
    **b. Active Liveness Check** – Prompting a Customer to follow a randomly moving dot on the screen, the algorithm would monitor pupil movement to check if it has been done correctly.

7. Get Identity Documents: To enroll for Tier 2, a Customer needs to provide a means to verify all the details provided in Tier 0 and Tier 1. Tools used to verify this are usually Government approved IDs, which can be International Passport, Driver's Licence, Citizenship IDs (e.g., NIMC), etc.
8. Get Previous Names, if required: Due to name change, which is most peculiar with women whose marital status has changed, one may or may not request for this detail.
9. Verify Customer Address: Moving a Tier higher on which further extends the customer transaction limits. All provided details would need to be verified. Starting with address and this can be verified today using utility bills, but this is no longer sufficient.
10. Verify Identity Documents: Documents provided are verified against National databases to asset authenticity.

# Digital Onboarding for Non-Individuals

Digital onboarding for non-individuals poses a different set of challenges for the financial institutions because of the high number of parties involved and by the fact that the non-individual itself is a distinct and separate legal entity. These problems are resolved by the adoption of certain principles:

1. A non-individual will always be represented by individuals who have legal or fiduciary rights to do so
2. Every representative must be verified up to the same tier of KYC that the non-individual must be or much more
3. A minimum number of representatives must be verified before the onboarding underlying non-individual entity can be completed

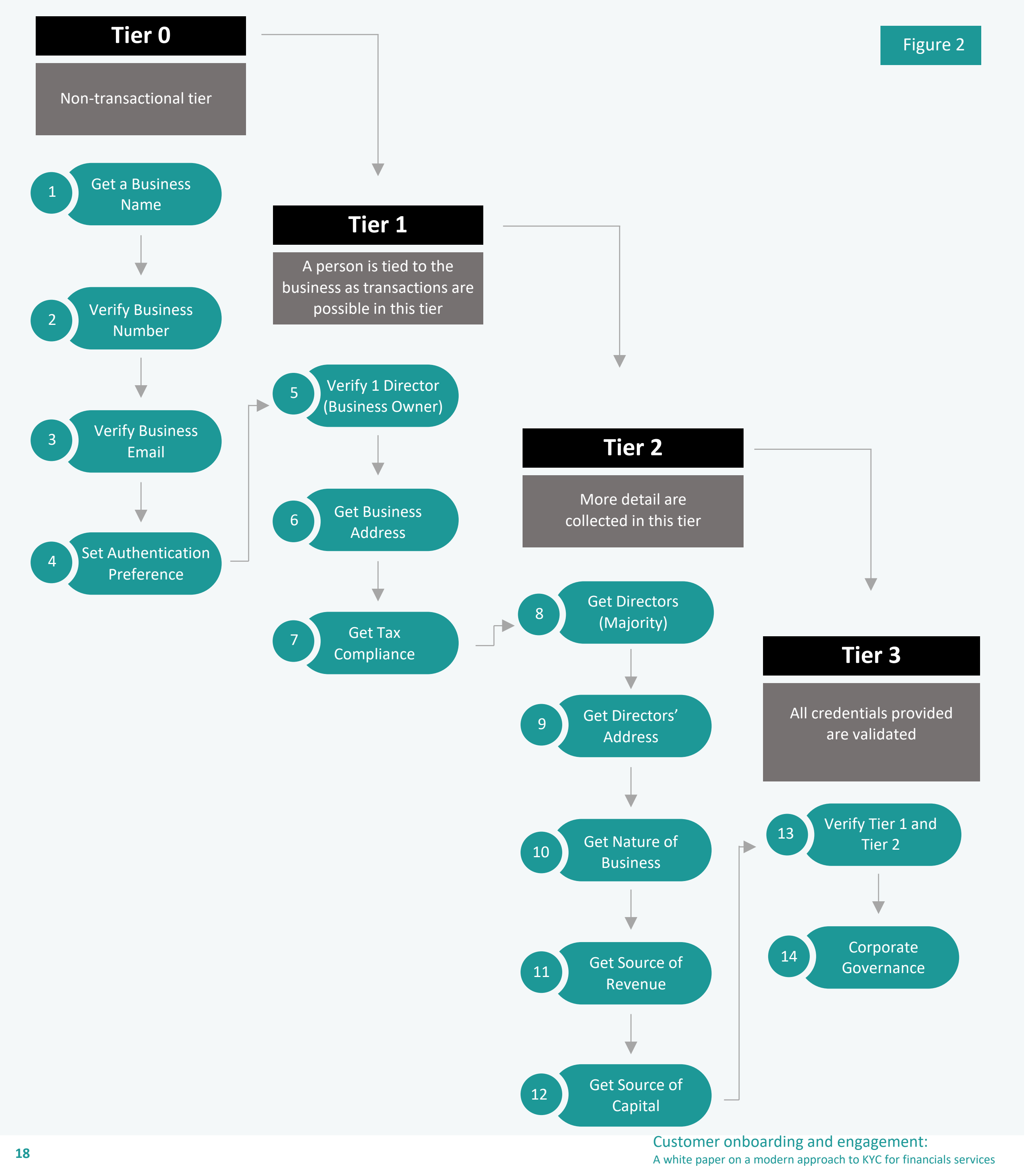



Figure 2

### Understanding the Onboarding Customer Journey for a Non-Individual

1. Get Business Name: Inputs Business Name inclusive of Company identification number.

2. Get Business Number: Input Business phone number which can be verified by
    a. Sending an OTP to the phone number to complete the onboarding process
    b. Initiating a voice call and OTP is given to the customer on the call to complete the onboarding process

3. Get Business Email: Inputs Business email which can be verified by
    a. Sending an OTP to the email to complete the onboarding process
    b. Sending an embedded link that redirects the customer to the next phase of the onboarding process.

4. Set Authentication Preferences: Different authentication techniques are available today, and for most financial applications, multi-factor authentication is advised. **Multi-factor authentication** (MFA) is a security system that requires more than one method of **authentication** from independent categories of credentials to verify the customer's identity for a login or other transaction. There are generally three recognized types of authentication factors:
    **a. Type 1 – Something You Know –** includes passwords, PINs, combinations, code words, or secret handshakes. Anything that you can remember and then type, say, do, perform, or otherwise recall when needed falls into this category.
    **b. Type 2 – Something You Have –** includes all items that are physical objects, such as keys, smartphones, smart cards, USB drives, and token devices. (A token device produces a time-based PIN or can compute a response from a challenge number issued by the server.).
    **c. Type 3 – Something You Are –** includes any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification.

5. Verify 1 Director: Being a transactional Tier, one of the Business directors would need to undergo the Individual onboarding process for a Tier 1 Customer.

6. Get Business Address: Here, the Business Address is required in this stage but not mandatory to verify.

7. Get Tax Compliance: Based on regulatory requirements, all businesses are expected to be tax compliant. The tax Identification number is gotten in this stage but not necessarily verified.

8. Get Directors (Majority): To enroll for Tier 2, the majority of the Directors of the business would be expected to undergo the Individual Onboarding process for a Tier 1 customer. If a company has five directors, at least three should enroll.

9. Get Nature of Business: Input Nature of the business

10. Get Source of Capital: Input Source of Capital

11. Get Source of Revenue: Input Source of Revenue

12. Verify Tier 1 and Tier 2: Moving a Tier higher, which further extends the Business transaction limits. All provided details would need to be verified. Business-related documents like
    a. Licenses to verify the nature of business
    b. Proof of funds to verify capital
    c. Proof of Income to verify revenue
    d. Company incorporation documents to verify Directors and company details
    e. Tax Clearance to verify Tax clearance

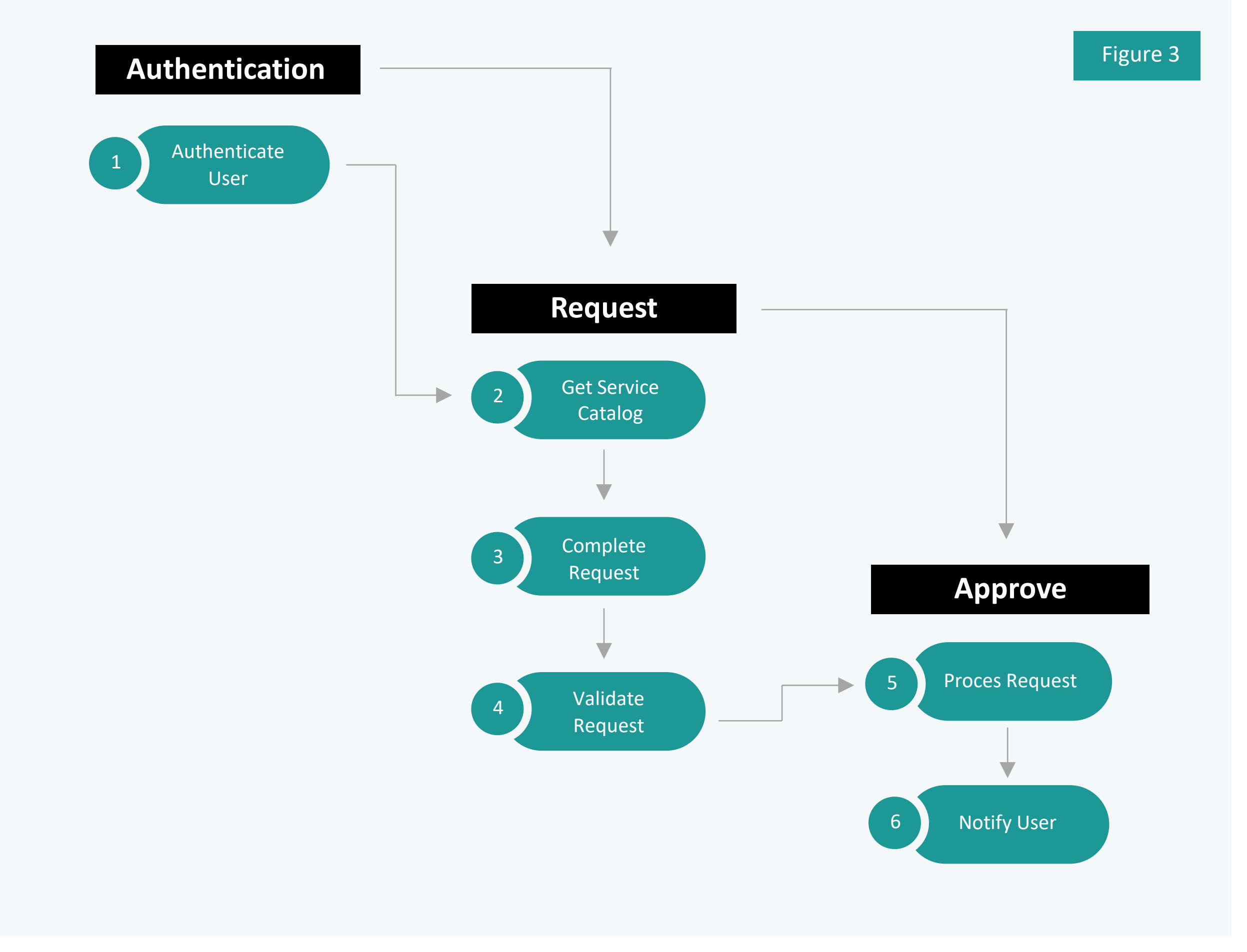
Documents provided are verified against National databases to asset authenticity.

13. Corporate governance: This is verified by reviewing policy and procedure documents of the business to verify there is a structure in place and the necessary regulatory enforcements and standards are abided to.

## Digital Customer Request

The digital journey for customer request describes the process where customers could require their financial services providers to make changes to their accounts, request new services, and/or report issues.

The journey described below represents a framework for the design of a secure process where customers are verified over digital channels, and the comfort of the authentication can provide a means by which subsequent requests made by the customers can be approved or effected by the financial services provider without physical paperwork.



### Understanding the Digital Request Customer Journey

1. Authenticate Customer: At the start of the journey, the customer must be authenticated on the digital channel of the financial services provider. Channel could be mobile, internet, or USSD banking. Some channels, such as ATMs, provide limited digital interactivity, which may limit the number and types of requests that could be made on them

2. Get Service Catalog: The channel will connect to the ERP or similar system to request the service catalog, a rich set of request options that the customer can make. The catalog would be determined by various rules such as the channel, profile of the customer, the KYC tier, etc.

3. Complete Request: The Customer is able to complete their request online, and over the channel, they are authenticated on. Also, the information that the channel already has of the customer should not be requested. For example, customers should not be asked to type in their names, phones, emails, etc.

4. Validate Request: Using the appropriate business and risk-based rules, the channel must validate the customer request. At this stage, once validated, the customer must have a certainty that the request has been made. No other additional information, which can be provided by the channel, should be requested by the customer. Customer authentication must be taken to be as valid, or even much more, than Customer wet-ink signature

5. Process Request: Validated requests from authenticated Customers are scheduled for implementation. Depending on the maturity of the financial institution or the process, the customer's request may be implemented manually and out of band

6. Notify Customer: The Customer must be informed by the outcome of the process within the stipulated time. While the request is still pending resolution or implementation, the channel must be able to show a pending status for such requests. Once an outcome has been reached, the customer must be informed via the channel, and also by at least one other means of communication such as by email or SMS.

## Engaging Customers Via Video Chats for Additional Verification

Quite often, there is a need to verify customer instructions, especially when they are out of character. Embedding a video chat into the digital channel creates a more secure and a smoother experience for the customer.

Video remains the best means of verification and can be part of mobile or web channels through the use of simple but sophisticated Software Development Kits (SDK).

To set up a call with a customer, the Customer Service Officer, or a representative of the financial services provider would have set up an appointment with the customer. Unlike telephony, video communication is more engaging and requires that customers be comfortable

# Authors

**Olowe, Adedeji**
adedeji@openbanking.ng
+234 703 413 8291

**Tommy, Unyime Sarah**
unyime@assurdly.com
+234 803 611 4421

**Popoola, Ayowole**
ayowole.popoola@fidelitybank.ng
+234 817 165 8023

# References

1. https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/issuance/id-verification/know-your customer#:~:text=KYC%20or%20KYC%20check%20is,who%20they%20claim%20to%20be.
2. https://m.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?Id=4354&Mode=0
3. https://fin.plaid.com/articles/kyc-basics/#:~:text=KYC%20laws%20were%20introduced%20in,means%20to%20deter%20terrorist%20behavior
4. https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/issuance/id-verification/know-your-customer
5. https://vikaspedia.in/social-welfare/financial-inclusion/know-your-customer-guidelines
6. https://www.trulioo.com/blog/kyc/
7. https://monzo.com/blog/2017/11/03/simple-signup-KYC
8. https://wup.digital/blog/digital-onboarding-banking/
9. https://www.barclays.in/content/dam/barclays-in/documents/download-forms/kyc/Importance_of_KYC.pdf