THOUGHT LEADERSHIP

JACKSON, ETTI & EDU

# DATA PRIVACY & KNOW YOUR CUSTOMER (KYC) REQUIREMENTS IN THE BANKING INDUSTRY:

## Unraveling The High-stakes Tensions In The Eke V. CBN's Case.


www.jee.africa

# Introduction

Banks play a vital role in the financial system by providing essential financial services to individuals and companies. They provide a secure place to deposit money as a financial services provider and control the flow of money to businesses that require the funds to grow and expand their businesses. The adoption of digital banking, along with the need for a stable and secure financial system, has necessitated the implementation of the Know Your Customer (KYC) process which is a mandatory procedure for verifying the identity and credentials of customers, for the primary purpose of preventing fraudulent activities and illicit practices that could undermine the stability of the financial system. However, with the introduction and evolution of digital banking, it is important to maintain a balance by effectively implementing KYC processes for customers and appropriately recognizing their privacy rights to prevent an avoidable conundrum. This article seeks to consider the convergence of data privacy and KYC measures in the Nigerian banking system by exploring the recent Nigerian court case of EKE v CENTRAL BANK OF NIGERIA,[1] which ignited the debate about the intersection of privacy rights and KYC regulations in the financial services sector.

## BANKING, EVOLUTION OF DIGITAL BANKING AND DATA PRIVACY

Basically, banking is the business activity of accepting deposits from the public, safeguarding those funds, and using them to provide loans, facilitate payments, and offer financial services.

According to the Banks and Other Financial Institutions Act (BOFIA) 2020, Banking is defined as "the business of receiving deposits on current account, savings deposit account or other similar account, paying or collecting cheques, drawn by or paid in by customers; provision of finance consultancy and advisory services relating to corporate and investment matters, making or managing investments on behalf of any person whether such businesses are conducted digitally, virtually or electronically only or such other business as the Governor may, by order publish in the gazette, designate as banking business.[2]

[1] *Unreported. FHC/L/CS/1281/2023 – Honourable Justice Nnamdi Dimgba of the Federal High Court, Lagos Division.*
[2] *Section 2 of the Banking and other financial Institutions Act, 2020*

It is important to note that the provision of banking services is heavily regulated by the Central Bank of Nigeria (CBN). Consequently, only licensed entities can provide any form of banking services in Nigeria whether traditional or digital or both.

### Digital Banking

Digital banking refers to the use of digital technologies especially the internet and mobile devices to deliver banking services and manage financial transactions without the need to visit a physical bank branch. Examples are Traditional Banks offering online/mobile banking or fully digital or Neobanks offering full digital services without a physical outlet/branch.[3]

Digital Banking evolution has come a long way since the days when transactions could only be conducted in the traditional physical centres. It transcends the banking system beyond the physical financial centres to a virtual online banking system that is internet enabled and offers it users a-round-the-clock access to financial services, therefore enhancing speed and reduced transaction cost thereby making banking faster, more convenient, and accessible, aligning with the shift toward a more connected and tech-driven financial world. In fact, globally, it is estimated that the integration of digital banking services results in a 20% reduction banking operational cost.[4]

As digital banking continues to expand, financial institutions must address complex security challenges while maintaining operational efficiency. Robust data privacy strategies, including encryption, authentication controls, and regulatory compliance, help mitigate risks and strengthen cybersecurity defence. Protecting banking data privacy is essential for preventing fraud, securing transactions, and ensuring long-term customer confidence.

### Data Privacy

Data privacy in banking refers to the protection of sensitive financial and personal information collected, stored, and processed by financial institutions. It also refers to the right of individuals to control how their personal information is collected, used, shared, and stored by organizations, governments, or other entities. Banks handle vast amounts of customer data, including account details, transaction history, personally identifiable information (PII), and biometric authentication records. Data privacy is about respecting and safeguarding people's personal information, ensuring it's handled responsibly and securely.

It is the duty of financial institutions to ensure strict policies are implemented, security measures, and compliance with regulatory standards are observed to prevent unauthorized access, data breaches, or misuse of financial information.

Some importance of Data Privacy and protection are:

- Protection of individual rights and freedom.
- Prevention of identity theft and fraud.
- Building trust between users and organizations.
- Ensuring compliance with laws and regulations.

*3 'Challenges of digital privacy in banking organizations' by Okechukwu Innocent Ogudebe, Walden University.*
*4 ibid*

### The KYC Regime in Nigeria

Financial institutions handle vast amounts of sensitive customer information, making data privacy in banking a critical priority. In view of the flow of funds within the financial system, there is a need to curtail illicit practices such as money laundering, terrorism financing, and other fraudulent practices. Therefore, there is no doubt that digital banking activities may expose bank and their customers to fraudulent activities. This is why consumers continue to demand increased support against fraudulent activities like identity theft and identity fraud as the goal is to compromise a customer's right to digital privacy with a view to facilitating financial fraud.

To curb the rise of fraudulent activities and ensure smooth, secure transactions within the Nigerian banking system, the CBN as part of its oversight function over financial institutions, has outlined mandatory requirements for banks to conduct KYC procedures on their customers to verify their identity and legitimacy. The mandatory requirements ensure the following:

a. Assist banks perform risk assessment by identifying the previous financial history and assets owned
b. Limit fraud that result mainly due to hiding of identity
c. Prevent money laundering and other anti-social activities
d. Bring stability and investment to the country, as it makes the financial framework more trustworthy and less risky
e. Decrease uncertainty by allowing financial institutions to lend more to customers and increase their profitability.

## THE EKE V CBN CASE AND THE PRIVACY DEBATE

It is agreed that data privacy and compliance with KYC requirement are important tools for safeguarding and protecting banks and customer against risks relating to financial fraud. However, it is also agreed that there can exist competing priorities between data privacy and KYC particularly where private and confidential information likely to comprise the privacy of a customer is demanded by a financial institution. This is the crux of the Eke vs CBN case.

The CBN under section 6 (iv) of its Customer Due Diligence Regulations of 2023 directed that certain information be obtained from customers of financial institutions including the collection and verification of customers' social media handles as a reflection of its commitment in keeping with the pace of technological advancement.

The CBN also explained that this directive will help the financial institutions gain comprehensive and holistic understanding of its customer and better evaluate the potential risk associated with money laundering, terrorism financing, and proliferation financing.

The requirement to obtain the social media handles of customers was frowned at in many circles as it was seen as a violation of the privacy of the customers. The question was whether the CBN was permitting financial institutions to sacrifice the data security of its customers on the altar of safeguarding the exposure of the financial system to fraudulent activities and whether this was a breach of the constitutional rights of the customers.

## CASE SUMMARY

The case of EKE v CBN[5] was instituted by a Nigerian Lawyer named Mr. Chris Eke against the CBN, seeking a declaration inter alia that **Section 6(a)(iv) of the CBN Regulations**[6] was undemocratic, unconstitutional, null and void to the extent of its inconsistency with Section 37 of the Constitution.[7] The Court in its ruling delivered on May 16, 2024 by Honourable Justice Dimgba of the Federal High Court upheld the CBN regulation mandating social media handle collection during KYC processes. The Court rejected the plaintiff's contention that this infringed upon his privacy rights, reasoning that social media handles, similar to email addresses and phone numbers, were public communication tools, and requiring them did not constitute a privacy breach. In essence, the apex bank can enforce the regulation which requires financial institutions to demand customers' social media handles as part of normal bank customer due diligence.

## UNDERSTANDING THE CONCEPTS OF PRIVACY RIGHTS AND KYC PROCEDURES

### Privacy Rights:

The concepts of privacy rights and know your customer (KYC) procedures are two different concepts that can sometimes conflict with each other. The conflict is mostly visible in the context of private data collection in the financial services sector.

Privacy rights pertain to an individual's right to control their personal information and how it is collected, used, or shared. This includes the right to keep certain information confidential and restrict its disclosure to others.

5 *'Unreported. FHC/L/CS/1281/2023 – Honourable Justice Nnamdi Dimgba of the Federal High Court, Lagos Division.*
6 *Section 6(a)(iv) of the Central Bank of Nigeria Customer's Due Diligence Regulation, 2023.*
7 *Constitution of the Federal Republic of Nigeria, 1999 as amended.*

For context, S. 37 of the Constitution of the Federal Republic of Nigeria, as amended provides:

> ***''The privacy of citizens, their homes, correspondence, telephone conversation and telephone conversations and telegraphic communication is hereby guaranteed and protected''.***

Privacy right is a fundamental human right that protects individuals from unwarranted intrusion into their personal lives. They are essential for maintaining autonomy, dignity, and freedom from unwarranted surveillance. The Supreme court in trying to expatiate on the gamut of the privacy rights of citizens under s. 37 held thus:

> ***"The meaning of the term "privacy of citizens" is not directly obvious on its face. It is obviously very wide as it does not define the specific aspects of the privacy of citizen it protects. A citizen is ordinarily a human being constituting of his body, his life, his person, thought, conscience, belief, decisions (including his plans and choices), desires, his health, his relationships, character, possessions, family etc. So, how should the term, privacy of the citizen be understood? Should it be understood to exclude the privacy of some parts of his life?***

This explains why the Supreme Court in **Medical and Dental Practitioners Disciplinary Tribunal v. Okonkwo**[8] while trying to give a constitutional interpretation to the meaning of 'privacy' as used in the constitution adopted a non-restrictive and liberal approach when it held that;

> ***the right to privacy implies a right to protect one's thought, conscience or religious belief and practice from coercive and unjustified intrusion and one's body from unwarranted invasion."*** *Per EMMANUEL OLAYINKA AYOOLA, JSC (Pp. 45-46, paras. G-F) Also see* ***A-G Lagos State V Eko Hotels Ltd & Anor (2006) 9 SC 46***

Even the trial court in the above matter while stating the scope of the right to privacy under S. 37 adopted the non-restrictive approach. This can be seen from its holding that the right includes 'privacy in private family life and incidental matters'.

The right to privacy is also enshrined in several other international and domestic statutes including but not limited to the Universal Declaration of Human Rights, Nigerian Data Protection Act, 2023, etc.

**Legal attributes of the privacy rights include -**

a. **Autonomy of personal privacy:** Privacy rights are essential for individual autonomy and self-determination. This concept allows individuals to make choices about how their personal information is collected, used, and shared, enabling them to maintain control over their own lives.

b. **Dignity and respect:** Privacy rights uphold the dignity and respect of individuals by safeguarding their personal information from unauthorized access, misuse, or exploitation. Respecting privacy helps prevent individuals from feeling vulnerable or exposed.

[8] *2001 LPELR 1856 SC*

c. **Freedom of expression and thought:** Privacy rights support freedom of expression and thought by creating a safe space for individuals to develop ideas, beliefs, and opinions without fear of judgment or interference. This fosters creativity, diversity, and intellectual exploration.

d. **Security and safety:** Privacy rights contribute to individuals' security and safety by safeguarding their personal data from identity theft, fraud, cybercrime, and other malicious activities. Protecting privacy helps prevent harm and promotes trust in online and offline interactions.

e. **Confidentiality in relationships:** Privacy rights protect confidential communications and relationships, such as those between doctors and patients, lawyers and clients, and individuals and their families. Upholding privacy in these contexts fosters trust and promotes open communication.

f. **Fairness and equality:** Privacy rights promote fairness and equality by preventing discrimination, profiling, and unfair treatment based on personal characteristics or information. Protecting privacy helps ensure that individuals are judged on their merits and actions, rather than on irrelevant factors.

In principle, the rationale behind privacy rights is grounded in principles of autonomy, dignity, freedom, security, confidentiality, fairness, and equality. Upholding privacy rights is essential for protecting individuals' personal freedom and liberty, fostering trust in society, and maintaining a beneficial balance between personal privacy and legitimate interests.

Individual privacy rights are fundamental. They encompass the right to control personal information, including collection, use, and disclosure. Section 37 of the Nigerian Constitution guarantees the privacy of citizens regarding communication, correspondence, and homes. Broader legal interpretations recognize privacy as encompassing aspects of personal life, relationships, and thoughts.

**KYC Procedures:**

KYC procedures refer to a set of procedures employed by a bank and other financial institutions to verify the identity of their customers and assess their potential risks. It is essentially a means of making sure that the customer is who they say they are. These typically involve collecting identification documents, proof of address, and sometimes, social media handles, as in the EKE v CBN case.

The KYC process typically involves a few steps, such as identity and address verification which necessarily requires the customer to provide some form of identification document, such as a passport or driver's license and, as the case in hand, their social media account; proof of address, such as a utility bill or bank statement.

**Rationale behind KYC procedures include -**

a. **Security of the financial sector:** the primary essence of customer is the prevention of financial crimes. The primary reasons for KYC regulations is to prevent money laundering, terrorist financing, fraud, and other financial crimes. By verifying the identity of customers and understanding their financial activities, businesses can detect and deter illicit transactions.

b. **Risk Management:** KYC helps bolster financial institutions assess the risk associated with their customers. By understanding who their customers are, businesses can better evaluate the level of risk they pose in terms of potential financial crimes or regulatory violations in line with international best practices.

c. **Regulatory compliance:** KYC regulations are often mandated by regulatory authorities to ensure that businesses comply with anti-money laundering (AML) and counter-terrorist financing (CTF) laws. Compliance with KYC requirements help businesses avoid legal and financial penalties.

d. **Protecting Reputation:** Implementing robust KYC procedures can help businesses protect their reputation by demonstrating a commitment to integrity and compliance with regulatory standards. This can enhance trust with customers, investors, and regulators.

e. **Enhancing Financial System Integrity:** KYC regulations contribute to the overall integrity of the financial system by reducing the risk of illicit financial activities that could undermine the stability and credibility of financial institutions.

f. **Customer Protection:** KYC measures can also help protect customers from fraudulent activities, identity theft, and unauthorized transactions by ensuring that their identities are verified, and their financial information is secure.

It is pertinent to note that by virtue of the Central Bank of Nigeria (CBN) establishment Act, CBN is charged with the responsibility or acting in a supervisory capacity and intervene in the operations of a bank where it is considered to be in the public interest to do so. This is seen in the case of **Omoyeni v. CBN & Ors.**[9]

There is no doubt that the CBN Act and the BOFIA empowered the CBN to make guiding principles to regulate the activities of banks and other financial institutions. There is no gainsaying that this regulatory and supervisory role extends to the power to make regulations regulating Know-Your-Customer procedures.

The big question is whether it can be said to be in the public interest to require banks or other financial institutions to obtain the social media handles/accounts from the customer against the customer's will.

In the whole, the rationale behind KYC regulations is focused on promoting financial integrity by compliance with regulations, risk management, and customer protection. By implementing effective KYC procedures, businesses can contribute to a safer and more secure financial environment for all stakeholders.

### Evaluation of the conflict between privacy rights and KYC procedures

The conflict between KYC regulations and privacy rights is a complex issue that requires careful consideration. On the one hand, KYC regulations are in place to prevent money laundering, terrorism financing, and other financial crimes by requiring businesses to verify the identity of their customers and protect the integrity of the financial system.

*9 [2015] LPELR – 25789(CA)*

On the other hand, privacy rights are fundamental rights that individuals must protect their personal information from being misused or disclosed without their consent. Some argue that KYC requirements can infringe on the privacy rights by collecting and storing sensitive personal data, potentially putting individuals at risk of identity theft or unauthorized access.

The conflict becomes even more acute where banks and other financial institutions while carrying out their due diligence on customers via KYC procedure go overboard by demanding personal information which a customer considers unnecessary or private. The danger of this is that it may lead to data breaches or unauthorized use of sensitive information. While KYC is essential for preventing financial crimes, it must be balanced against individual privacy rights and private data breaches.

**Striking a balance and recommendations**

Finding a balance between robust KYC procedures and individual privacy rights is crucial. It is important for financial institutions to implement KYC procedures in a way that complies with data protection laws and respects individuals' privacy rights. This can be achieved through measures such as data minimization, encryption, secure storage, and ensuring transparency in how customer data is used and protected. Also, operating a harmonized Customer Identification Program (CIP) which involves the collection and verification of information such as name, date of birth, address, and identification number.

Customers must be informed and consent to the collection and use of their personal data. Regulators and lawmakers should establish clear guidelines to ensure that KYC compliance does not come at the expense of privacy rights. Social security number like the BVN, NIN and the likes should be sophisticated and technologically developed to give room for zero or very low margin of error. This will help restore public confidence in the financial sector and reduce any form of tension spanning from the apprehension about potential privacy rights breaches.

If a balance between these two conflicting concepts is struck, we can promote a safer and more trustworthy financial system that respects individual autonomy and dignity.

**Here are some recommendations -**

a. **Data Minimization:** Financial institutions should only collect essential KYC information.

b. **Data Security:** Implementing strong encryption, secure storage, and clear data protection policies are paramount.

c. **Transparency:** Customers should be informed about how their data is used and protected.

d. **Customer Consent:** Obtaining informed consent for data collection is essential.

e. **Harmonized Customer Identification Programs (CIP):** Standardized programs for collecting and verifying core information like names, addresses, and identification numbers can streamline KYC processes.

f. **Technological Solutions:** E-KYC (electronic KYC) and other innovative solutions can facilitate KYC compliance while respecting privacy.

# Conclusion

The EKE v CBN's case highlights the ongoing tension between privacy and security in the financial sector. Striking a balance through robust data protection measures, clear regulations, and technological advancements is vital. This will help foster a financial system that is both secure and respectful of individual privacy rights.

In the final analysis, both KYC regulations and privacy rights play important roles in maintaining the integrity of the financial system while safeguarding individuals' personal information. Finding a middle ground that upholds both objectives is key to addressing the conflict between KYC and privacy rights. Again, the adoption of e-KYC and innovative solutions will help balance regulatory compliance with the need to respect the individual's basic right to privacy.

However, it will be interesting to see the unfolding of this matter (CBN v. EKE) and to see how the appellate court will consider it knowing fully well that 'privacy rights' is a constitutional issue which in the author's view involves a substantial question of law as envisaged in section 295 of the CFRN, 1999 as amended.

## AUTHOR

**Henry Obinna Obidinma**
Associate

# KEY CONTACT

For further information, kindly reach the contact below:


## Kunle Soyibo

Partner, Head of Financial Services Sector

kunle.soyibo@jee.africa



**Telephone**
+234 (02) 014626841/3,
+234-(02) 012806989

**Email**
jee@jee.africa

**Victoria Island**
RCO Court,
3-5 Sinari Daranijo Street,
Victoria Island, Lagos, Nigeria.

**Abuja**
42, Moses Majekodunmi Crescent.
Utako, FCT, Abuja

**Ikeja**
1st floor, ereke house, Plot 15,
CIPM Avenue
CBD Alausa Ikeja
Lagos Nigeria

**Accra**

**Yaoundé**

**Harare**