YourLawArticle

Open Access Law Journal, ISSN (O): 3049-0057

Editor-in-Chief – Prof. (Dr.) Amit Kashyap; Publisher – Reet Parihar

KYC : It's Significance, Functionality And Regulatory Legal Framework

Ashok N. Kotangle , Researcher , Department of Law, University of Mumbai

Published on: 15th October 2025

Abstract

Know Your Customer (KYC) is a regulatory, preventive, and risk-management framework adopted globally to verify customer identity, ensure financial transparency, and combat economic crimes such as money laundering, fraud, tax evasion, and terrorist financing. The concept, rooted in early foreign exchange regulations and strengthened after liberalization, has evolved into an essential compliance mechanism for financial institutions, banks, and digital platforms. KYC serves multiple objectives: safeguarding national and economic interests, promoting accountability, preventing misuse of financial systems, and aligning with international standards like those of FATF, IMF, and the UN.

The nature of KYC is multidimensional—administrative, legal, preventive, and regulatory—enforced through documentation norms, customer due diligence, and continuous monitoring. In India, its legal foundation stems from the Foreign Exchange Regulation Act (FERA), its successor FEMA, and the RBI's Master Directions. Key judicial interventions, including Aadhaar cases (2017, 2019), the FinCEN v. Ripple Labs case (2015), and R. v. NatWest Bank (2021), demonstrate how courts have shaped the contours of customer verification, privacy, proportionality, and data usage. KYC also extends to digital payments, cryptocurrency transfers, and non-banking sectors under evolving jurisprudence.

By mandating identity validation, address proof, risk profiling, and transaction tracking, KYC helps institutions prevent fraudulent conduct, maintain data integrity, and ensure responsible financial participation. Overall, KYC has transitioned from a compliance formality to a core instrument of national security, regulatory governance, and global financial integration.

KEYWORDS: - KYC compliance, money laundering, RBI regulations, customer due diligence, financial fraud prevention

INTRODUCTION:

KYC stands for know your customer. It is a process by which bank, financial institution, and other regulated entities verify the identity and address of their customer before providing services. It involves collecting and validating documents like ID proof and address proof to prevent fraud, money laundering, and other illegal activities. KYC ensures that companies understand who their customers are and can assess the risks associated with them, making financial systems safer and more transparent. The main objective is to ensure that the client is genuine and not involved in any illicit or illegal activities such as money laundering, fraud, or terrorism financing. It is no longer a one-time compliance requirement but a continuous process that includes regular monitoring, risk assessment, and customer due diligence throughout the customer lifecycle. Long term implementation of KYC helps financial institutions build trust with customers, comply with ever evolving regulatory requirements, and effectively manage risks.[1]

AIMS AND OBJECTIVE OF KYC:

1. **Identity Verification**
   - Ensures that the customer is a real, identifiable person and not using a fake identity. Identity verification is the process of confirming that the personal details and documents provided by a customer are genuine and belong to the person claiming them. It is the first and most important step in the Know Your Customer (KYC) procedure.

   - **Purpose:**
     1. To ensure that the customer is a real and legitimate individual or entity, in case of companies.
     2. To prevent criminals from using false or stolen identities for illegal activities.

   - **Methods of Identity Verification:**
     1. Official Documents i.e. Passport, Aadhaar card, PAN card, Voter ID, Driving License, etc.
     2. Biometric Verification i.e. Fingerprints, iris scan, or facial recognition especially with Aadhaar e-KYC.
     3. Digital Verification i.e. OTP based authentication linked to mobile numbers and email IDs.
     4. In-person Verification i.e. Physical presence for certain high value transactions.
   - **Importance:**

[1] Navi Technologies, 'KYC Full Form' (Navi, 2025) https://navi.com/blog/kyc-full-form/ accessed 10 January 2025.

1. Builds trust between customer and institution.
2. Helps in tracking financial activities to prevent fraud, money laundering, or terrorism financing.
3. Ensures compliance with legal and regulatory frameworks.

1. **Prevention of Financial Crimes**

- Helps combat money laundering, terrorist financing, fraud, and other illegal financial activities. One of the main objectives of KYC (Know Your Customer) is to prevent financial crimes such as money laundering, terrorist financing, fraud, identity theft, and corruption. By verifying the identity and background of customers, financial institutions can ensure that their services are not misused for illegal purposes.
- **How KYC Prevents Financial Crimes:**

  1. Customer Due Diligence (CDD) such as proper verification of identity, address, and source of funds helps detect suspicious customers.

  2. Monitoring Transactions such as continuous monitoring ensures unusual or high value transactions are reported.

  3. Reporting Suspicious Activity such as institutions are legally required to file Suspicious Transaction Reports (STRs) to authorities.

  4. Screening Against Watchlists such as customers are screened against blacklists, sanction lists, and politically exposed persons (PEPs).

  5. Risk Assessment such as identifying high-risk customers reduces chances of financial systems being used for illegal activities.
- **Importance:**

  1. Protects the financial system from abuse.
  2. Helps in national and global security by curbing terrorist financing.
  3. Builds public trust in banks and financial institutions.
  4. Ensures compliance with laws like the Prevention of Money Laundering Act (PMLA), 2002 and guidelines from RBI, SEBI, FATF, etc.

- **Regulatory Compliance** [2]

- Mandatory under laws such as the Prevention of Money Laundering Act (PMLA), 2002 in India and guidelines issued by RBI, SEBI, IRDAI, etc. Regulatory compliance means following the rules, laws, and guidelines set by government and regulatory authorities. In the case of KYC, financial institutions are legally required to verify the identity of their customers before offering services.

[2] Akhilesh S Dubey, *Treatise on Prevention of Money Laundering Act, 2002* (2nd edn, 2025)

- **Why KYC is Required for Compliance:**

1. Legal Mandate in India, KYC is compulsory under the Prevention of Money Laundering Act (PMLA), 2002 and rules framed by RBI, SEBI, IRDAI, and other regulators.
2. Global Standards in international bodies like the Financial Action Task Force (FATF) have recommended strict KYC norms to fight money laundering and terrorist financing.
3. Institutional Responsibility in Banks, insurance companies, mutual funds, and NBFCs must collect and verify customer details to avoid penalties.
4. Transparency & Accountability, ensures all transactions are traceable and legal.

- **Importance:**

1. Protects financial institutions from legal risks and heavy fines.
2. Ensures the financial system is not used for illegal activities.
3. Builds trust and credibility with customers and regulators.

4. Risk Management [3]

- Allows institutions to assess the risk profile of the customer and prevent misuse of financial systems. Risk management means identifying, assessing, and reducing potential risks that may arise from dealing with customers. In KYC, it refers to protecting banks and financial institutions from risks such as fraud, money laundering, terrorist financing, and reputational damage.

- **How KYC Helps in Risk Management:**

1. Customer Risk Profiling such as customers are categorized as low-risk, medium-risk, or high-risk based on their background, source of funds, and transaction patterns.
2. Enhanced Due Diligence (EDD) such as extra checks are done for high-risk customers like politically exposed persons (PEPs) or foreign clients.
3. Transaction Monitoring such as continuous observation helps detect suspicious or unusual activities.
4. Preventing Identity Fraud such as proper verification ensures criminals cannot misuse false or stolen identities.
5. Minimizing Legal and Financial Risk in Compliance with KYC rules protects institutions from penalties, fines, and loss of reputation.

- **Importance:**

[3] KYC AML Guide, 'Risk Management in KYC' (KYC AML Guide, 2025) https://kycaml.guide/blog/risk-management-in-kyc/ accessed 10 January 2025.

1. Safeguards institutions from financial losses.
2. Protects customers from identity theft and fraud.
3. Maintains the stability of the overall financial system.
4. Helps regulators track and prevent criminal activities.

5. **Transparency in Transactions**

- Ensures proper tracking of funds, making financial systems more accountable and trustworthy. Transparency in transactions means that all financial dealings are clear, traceable, and verifiable. KYC ensures that every customer's identity and financial activity are properly recorded, which reduces the chances of hidden or illegal transactions.

- **How KYC Promotes Transparency:**

1. Verified Identity- Customers are linked to valid documents (Aadhaar, PAN, Passport, etc.), ensuring accountability.
2. Clear Audit Trail i.e. every transaction can be traced back to its source and beneficiary.
3. Prevents Anonymous Dealings i.e. stops the use of fake or duplicate identities in the financial system.
4. Monitoring Mechanism i.e. regular checks and reporting of suspicious transactions improve visibility.
5. Disclosure of Beneficial Ownership i.e. ensures that the real owner behind accounts or companies is known.

- **Importance:**

1. Builds trust between customers and financial institutions.
2. Helps regulators track illegal or suspicious activities.
3. Prevents misuse of funds for crimes like money laundering or terrorism.
4. Creates a fair and accountable financial system.

6. Customer Protection[4]

- Safeguards customers from identity theft, unauthorized transactions, and misuse of their accounts. Customer protection refers to safeguarding individuals from financial fraud, identity theft, and misuse of their accounts. KYC plays a vital role in protecting customers by ensuring that only genuine and verified persons can use banking and financial services.

---

[4] Gagandeep Singh, *The KYC Handbook: Mastering Customer Due Diligence* (7 July 2025).

- How KYC Ensures Customer Protection:

1. Prevents Identity Theft i.e. verification of official documents prevents criminals from opening accounts in someone else's name.
2. Secures Accounts i.e. proper authentication (biometrics/OTP) reduces chances of unauthorized access.
3. Detects Fraudulent Transactions i.e. continuous monitoring helps in identifying suspicious activities in customer accounts.
4. Protects Against Financial Loss i.e. Customers are less likely to suffer losses due to fraud or fake transactions.
5. Builds Confidence i.e. Customers trust institutions more when they know security measures like KYC are in place.

- **Importance:**

1. Enhances customer safety in the digital financial world.
2. Strengthens trust between banks and customers.
3. Ensures fair practices and protects the rights of customers.
4. (KYC is a shield for customer protection, ensuring their identity, money, and trust remain secure.)

7. Global Standard Practice[5]

- KYC is a part of international best practices recommended by the Financial Action Task Force (FATF) to maintain integrity in financial systems. KYC (Know Your Customer) is not just a national requirement but a global standard practice adopted across the world to maintain integrity in financial systems. Almost all countries mandate KYC norms in line with international guidelines.
- Basis of Global Practice:
  1. Financial Action Task Force (FATF) i.e. An inter-governmental body that sets international standards for anti–money laundering (AML) and counter-terrorist financing (CFT).
  2. Basel Committee on Banking Supervision i.e. Recommends strong customer due diligence measures for global banking safety.

[5] Persona Identities Inc, 'KYC Best Practices for Global Compliance' (Persona Blog, 2025) https://withpersona.com/blog/kyc-best-practices-for-global-compliance accessed 10 January 2025.

3. International Organizations like World Bank, IMF, and OECD promote KYC compliance for financial stability and transparency.

- **How It Works Globally:**
  1. Standardized procedures for identity verification, due diligence, and reporting suspicious transactions.
  2. Risk-based approach to categorize customers (low, medium, high risk).
  3. Cross-border cooperation between financial institutions to combat global crimes.
- **Importance:**
  1. Prevents international money laundering and terrorist financing.
  2. Protects global financial systems from abuse.
  3. Ensures smooth functioning of cross-border banking, trade, and investments.
  4. Builds trust among global investors and institutions.

NATURE OF KYC[6]:

The nature of KYC refers to its fundamental characteristics, purpose, and how it functions within financial and regulatory systems. It is both preventive and regulatory in nature.

1. **Regulatory in Nature:**

KYC is a mandatory legal requirement under laws related to Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT). Enforced by financial regulators e.g., RBI, SEBI, FATF guidelines, etc. The Know Your Customer (KYC) process is inherently regulatory in nature, meaning it is primarily driven by laws, regulations, and guidelines imposed by governments and financial authorities worldwide. This regulatory framework aims to ensure that financial institutions and other regulated entities operate transparently, responsibly, and without facilitating illegal activities such as money laundering, terrorist financing, fraud, and tax evasion.

2. **Ongoing Process:**

KYC is not a one-time activity. It involves periodic updates, monitoring transactions, and re- verifying information as needed. involves regularly updating and monitoring customer information, behaviour, and risk profile throughout the business relationship. This ensures that the institution maintains up-to-date knowledge of its customers to detect and prevent suspicious activities like money laundering, fraud,

[6] Barclays India, 'Importance of KYC' (Barclays) https://www.barclays.in/content/dam/barclays-in/documents/download-forms/kyc/Importance_of_KYC.pdf accessed 9 January 2025.

or financing terrorism.

3. **Customer-Centric:**

Focuses on understanding the customer's identity, financial behaviour, and the purpose of their financial relationship. The concept of Customer Centric KYC places the customer at the heart of the Know Your Customer process. Instead of being a mere compliance obligation or a bureaucratic hurdle, KYC becomes an experience that respects, protects, and values the customer throughout their journey. Over the long term, as financial services evolve with technology and regulatory demands increase, making KYC customer-centric is essential to balance regulatory compliance with superior customer experience.

4. **Documentation-Driven:**

Relies heavily on valid documentation such as government issued ID, address proof, and sometimes financial or business documents. Know Your Customer (KYC) is a fundamental compliance process that requires customers to submit specific documents to verify their identity, address, and sometimes financial status. This process is said to be "documentation driven" because it relies heavily on official documents to establish and validate a customer's identity and risk profile. In the long term, while KYC processes have become more digital and automated, documentation remains a central element specially in regulated environments where compliance, auditability, and due diligence are critical

5. **Technology-Enabled:**

Increasingly done through digital platforms using e-KYC, biometrics, and AI to simplify and speed up the process. Technology enabled KYC uses digital tools and platforms to collect, verify, and manage customer identity and information electronically. Instead of submitting physical documents and waiting days for verification, customers can now complete the KYC process in minutes from their smartphones or computers. It leverages innovations such as AI, biometrics, OCR, video verification, blockchain, and secure APIs to streamline the process, minimize errors, and improve efficiency.

THE REGULATORY FRAMEWORK OF KYC[7]:

KYC (Know Your Customer) norms are governed by a comprehensive regulatory framework aimed at preventing financial crimes such as money laundering, terrorist financing, fraud, and identity theft. These regulations vary by country but share common international principles and guidelines.

1. **National Regulatory Frameworks**

- **Banking and Financial Sector Regulators**

Reserve Bank of India (RBI) India Issues detailed KYC guidelines for banks and financial institutions, including mandatory customer identification procedures and ongoing monitoring. Financial Crimes

[7] Benjamin Vogel and Jean-Baptiste Maillart, *National and International Anti-Money Laundering Law* (2024).

Enforcement Network (FinCEN) (USA) Oversees anti money laundering AML regulations in the US, including KYC requirements under the Bank Secrecy Act (BSA). Financial Conduct Authority (FCA) UK Regulates KYC and anti money laundering AML compliance for financial services firms. Other countries have similar bodies like the Monetary Authority of Singapore (MAS), Australian Transaction Reports and Analysis Centre (AUSTRAC), etc.

- **Anti-Money Laundering (AML) Laws**

AML laws typically embed KYC norms as a core requirement. Example- Prevention of Money Laundering Act (PMLA), 2002 in India mandates customer identification and record- keeping. Similar laws exist globally- USA PATRIOT Act (US), Proceeds of Crime Act (UK), etc.

- **Data Protection and Privacy Laws**

KYC involves handling sensitive customer data, so institutions must comply with privacy regulations such as General Data Protection Regulation (GDPR) (EU), California Consumer Privacy Act (CCPA) (USA) Various country specific data protection laws.

- **Important Case Laws on KYC in India**

(i) R. Rajagopal v. State Bank of India[8]

Issue: Denial of service for not furnishing Aadhaar for KYC. Can a superior officer (Chief Manager) be held culpable for failures in KYC document filing when the subordinate was responsible for obtaining them, especially when the superior had issued directions to ensure compliance? Is non-compliance with KYC documentation a serious misconduct sufficient to justify major penalties like dismissal / compulsory retirement, especially given financial loss? Held: Bank cannot deny services if customer provides other officially valid documents as per RBI Master Directions.

International Regulatory Bodies and Guidelines[9]

- Financial Action Task Force (FATF) : An intergovernmental body that develops international standards to combat money laundering and terrorist financing. FATF's 40 Recommendations provide a globally recognized framework for KYC and AML (Anti-Money Laundering) compliance. FATF recommends a risk-based approach to KYC, meaning institutions should tailor their due diligence based on the customer's risk profile.
- Basel Committee on Banking Supervision : Provides principles for effective banking supervision, including customer due diligence and KYC norms. Emphasizes risk management and internal controls for financial institutions.

[8] R Rajagopal v State Bank of India (Madras HC, 2019).
[9] KYC Hub, 'Global KYC Regulations: Key Requirements and Compliance' (KYC Hub, 2024) https://www.kychub.com/blog/global-kyc-regulations/ accessed 9 January 2025.

- United Nations Office on Drugs and Crime (UNODC) Supports international legal frameworks and conventions for anti-money laundering efforts, indirectly influencing KYC regulations.

1. **Danske Bank Money Laundering Scandal (Estonia, 2017–2019, EU)[10]**

Issue: Danske Bank's Estonian branch laundered ~€200 billion of suspicious Russian money. The core legal issue was Danske Bank's failure to prevent money laundering despite the scale of suspicious transactions and the warnings it received from employees and external auditors.

The bank was legally required to implement (anti–money laundering) AML procedures, KYC checks, and robust internal controls to detect suspicious activity. The lack of action exposed the bank to criminal liability under money laundering and financial crime laws in multiple jurisdictions.

Outcome: Bank faced multiple EU investigations, CEO resigned.

Principle: Cross-border (anti–money laundering) AML/KYC failures attract global enforcement.

2. **Standard Chartered Bank (2019, US & UK)**

   • Issue: Weak KYC & sanctions screening, especially for transactions with Iran. Standard Chartered Bank was found to have facilitated financial transactions for entities and individuals in Iran, Sudan, and Syria, which were subject to U.S. sanctions The bank was accused of processing U.S. dollar transactions for entities in these sanctioned countries, which violated U.S. OFAC regulations. U.S. sanctions prohibit U.S. financial institutions from engaging in transactions with these countries or entities that are subject to sanctions. To what extent did Standard Chartered systems fail to detect and prevent transactions involving sanctioned countries, and what level of responsibility does the bank bear for knowingly facilitating these violations?

   • **Outcome:** Fined $1.1 billion by US & UK regulators.

   • **Principle:** KYC compliance failures attract multi-jurisdictional penalties.

Global Standard Setter :

FATF (Financial Action Task Force) - Intergovernmental body (1989). Issues 40 Recommendations on AML/CFT - adopted by over 200 countries.

Requires customer due diligence (CDD), enhanced due diligence (EDD), and reporting of suspicious transactions (STR).

(a) United States

Bank Secrecy Act (BSA), 1970 - Core AML/KYC law.

[10] 'Danske Bank Case: Money Laundering Scandal' (Sanction Scanner, 2023) https://www.sanctionscanner.com/blog/danske-bank-case-money-laundering-scandal-11302 accessed 10 January 2025.

USA PATRIOT Act, 2001 - Strengthened AML/KYC post 9/11. Regulators:
FinCEN (Financial Crimes Enforcement Network) SEC (Securities and Exchange Commission)
OCC (Office of the Comptroller of the Currency)

(b) European Union

EU Anti-Money Laundering Directives (AMLD 1–6) - Framework for all member states.
General Data Protection Regulation (GDPR) impacts KYC data privacy.

(c) United Kingdom

Money Laundering Regulations 2017 (MLR). Regulator: FCA (Financial Conduct Authority).

(d) Other Countries

Singapore - MAS (Monetary Authority of Singapore) AML/KYC Notices. Australia - AUSTRAC (Australian Transaction Reports and Analysis Centre). UAE, Hong Kong, Canada - Similar FATF-aligned KYC/AML frameworks.

2. Core Components of the KYC Regulatory Framework

- **Customer Identification Program (CIP)**

Verification of customer identity at account opening using valid documents. Collection of basic information like name, date of birth, address, and identification number.

- **Customer Due Diligence (CDD)**

Assessing the customer's risk profile based on their background and transaction behaviour. Additional documentation or checks for higher-risk customers (Enhanced Due Diligence - EDD).

- **Ongoing Monitoring**

Continuous scrutiny of transactions and periodic updating of customer information.

- **Record Keeping**

Regulations specify retention periods for KYC records, typically 5–10 years after the end of the customer relationship.

- **Reporting Obligations**

Institutions must report suspicious transactions to regulatory authorities in compliance with (anti–money laundering) AML and CFT laws.

4. Recent Trends in KYC Regulatory Frameworks

1. Risk Based Approach : Regulators encourage tailored KYC based on customer risk rather than a one-size-fits-all approach.
2. Technology Driven Compliance : Guidelines for using digital identity verification, biometric

authentication, and AI for compliance.

3. Cross Border Collaboration : International cooperation to tackle global financial crimes.
4. Privacy and Data Security : Strengthened focus on protecting customer data during KYC.

KYC (Know Your Customer) norms are designed to prevent money laundering, terrorist financing, fraud, and financial crimes.

(a) **Statutory Basis**

Prevention of Money Laundering Act, 2002 PMLA Main legislation.

Rules under PMLA, 2005 Provides for KYC procedures, reporting obligations, and penalties.

(b) **Regulatory Authorities**

1. **RBI (Reserve Bank of India)-**

Issued the Master Directions on KYC (2016, updated frequently). Applies to banks, NBFCs, payment systems, etc.

Mandates Aadhaar, e-KYC, PAN, or other officially valid documents.

2. **SEBI (Securities and Exchange Board of India)-**

KYC for stock brokers, mutual funds, and capital markets.

Introduced KYC Registration Agencies (KRAs) to centralize KYC records.

3. **IRDAI (Insurance Regulatory and Development Authority of India)-** KYC norms for insurance policies to prevent benami illegal policies.
4. UIDAI (Unique Identification Authority of India) : Provides Aadhaar based e-KYC authentication for banks telecom.

5.Key Principles Emerging from Cases & Regulations

Aadhaar KYC is optional, not mandatory (except for PAN-ITR).It is an identification document issued by the Unique Identification Authority of India (UIDAI) that contains:

A 12-digit unique identification number
Your biometric data fingerprints, iris scan
Your demographic details name, date of birth, gender, address, etc.

- It is used for:

Proof of identity and address

Accessing government subsidies and schemes

KYC (Know Your Customer) for banking, SIM cards, etc. Filing income tax returns

1. **Justice K.S. Puttaswamy (Retd.) v. Union of India**[11]– The Aadhaar Case

   • **Facts:** Aadhaar scheme was challenged for violating the right to privacy.

   • **Issues:**

   Whether Aadhaar infringes the fundamental right to privacy.

   Whether Aadhaar should be mandatory for welfare schemes, PAN linking, bank accounts, mobile numbers, etc.

   • **Held:** Right to Privacy declared a fundamental right under Article 21. Aadhaar was upheld as constitutionally valid, but with restrictions: Mandatory for PAN linking and IT returns. Not mandatory for bank accounts, SIM cards, school admissions, private services.Authentication data cannot be retained beyond 6 months.

2. **Binoy Viswam v. Union of India**[12]

   • **Facts:**

   PAN was made mandatory to be linked with Aadhaar for income tax purposes.

   • **Held:**

   Court upheld Section 139AA of the Income Tax Act making Aadhaar-PAN linking mandatory.

3. **Lokniti Foundation v. Union of India**[13]

   • **Facts:** The case dealt with mandatory Aadhaar for mobile phone verification.

   • **Held:** Supreme Court directed the government to ensure proper verification of mobile subscribers but clarified Aadhaar cannot be made mandatory at that stage.

4. **Shanta Sinha v. Union of India**[14]

   • **Facts:** Petitioners challenged making Aadhaar mandatory for scholarships and mid-day meals.

[11]Justice KS Puttaswamy (Retd) v Union of India (2018) 10 SCC 1.
[12]Binoy Viswam v Union of India (2017) 7 SCC 59.
[13] Lokniti Foundation v Union of India BS827420 (SC 2016).
[14] Shanta Sinha v Union of India, Writ Petition (Civil) No 342 of 2017.

• Held: Supreme Court ruled that no child should be denied scholarships or mid-day meals for lack of Aadhaar.

ASSISTING THE GOVERNMENT, BANKS, AND CUSTOMERS IN KYC (LONG-TERM PERSPECTIVE):

Over the long term, the Know Your Customer (KYC) process plays a vital role in assisting three key stakeholders:

1. The Government
2. Banks and Financial Institutions
3. Customers (Individuals and Businesses)

1. Assisting the Government[15]

KYC is a powerful tool for governments in terms of regulation, security, and financial system integrity.

Benefits to the Government-

- Prevents Money Laundering and Terrorist Financing:

  KYC helps government agencies track financial activities and prevent misuse of the financial system for criminal or terror-related activities.

- **Supports Tax Compliance-**

  Proper identification through KYC helps authorities identify and monitor taxpayers, reducing tax evasion.

- Enhances Financial Transparency-

  Government can ensure that financial institutions operate within legal and ethical standards.

- Enables Effective Policy Making-

  Aggregated, anonymized KYC data helps in designing inclusive financial policies based on population demographics.

- Promotes National Security-

  Real-time monitoring and identification reduce the risk of financial crimes linked to national

[15] Government of India, 'KYC Awareness Document' (Ministry of Finance, 2023) https://cdnbbsr.s3waas.gov.in/... accessed 9 January 2025.

and international threats.

- Facilitates e-Governance and Direct Benefit Transfers (DBT)-

  KYC-enabled accounts ensure subsidies and benefits reach genuine, verified beneficiaries (e.g., Aadhaar-based KYC in India).

2. **Assisting Banks and Financial Institutions**[16]

   For banks and other financial entities, KYC is essential for risk management, compliance, and operational efficiency.

Benefits to Banks:

- Ensures Legal Compliance-

  KYC helps banks comply with national and international (anti–money laundering) AML and CFT laws, avoiding legal penalties.
- Reduces Fraud and Identity Theft-

  Strong identity verification lowers the risk of fraudulent account opening or transaction manipulation.
- Improves Risk Assessment and Management-

  Banks use KYC data to categorize customers by risk level and apply appropriate due diligence.
- Enables Safer Lending and Credit Decisions-

  Verified customer information helps in assessing creditworthiness and reducing non-performing assets (NPAs).
- Supports Better Customer Relationships-

  Understanding customer identity and financial behaviour enables personalized banking and targeted offerings.

- Facilitates Cross-Border Banking-

  Standardized KYC norms help in international banking and correspondent relationships.

[16] Persona, 'KYC in Banking' (2024) https://withpersona.com/blog/kyc-in-banking accessed 10 January 2025.

3. **Assisting Customers**[17]

While often viewed as a regulatory formality, in the long term, KYC protects and empowers customers.

Benefits to Customers:

- Secure Access to Financial Services-

  KYC allows individuals to open bank accounts, invest, get loans, and use insurance safely.

- Protection Against Identity Theft and Fraud-

  KYC helps prevent unauthorized use of personal data for opening fake accounts or illegal transactions.

- Eligibility for Government Schemes and Benefits-

  Verified KYC is required for receiving subsidies, scholarships, pensions, and other government services.

- Convenient Digital Banking-

  KYC enables seamless onboarding and usage of digital wallets, UPI, mobile banking, and fintech platforms.

- Faster and Smoother Transactions-

  Once verified, customers face fewer interruptions in future transactions, loan approvals, and investments.

- Enhanced Trust in the Financial System-

  Knowing that their bank follows strict KYC protocols gives customers confidence in the system's integrity.

CASE ANALYSES:

1. **Pragya Prasun & Ors. v. Union of India & Ors**.[18]

Case Name: Pragya Prasun & Ors. v. Union of India & Ors. & Amar Jain v. Union of India & Ors. (consolidated) W.P.(Civil) Nos.: 289 of 2024 (Pragya Prasun) and 49 of 2025 (Amar Jain)

Court: Supreme Court of India

Date of Judgment: 30 April 2025

- **Facts**

[17] Indian Institute of Banking and Finance, 'Anti-Money Laundering and KYC' (IIBF, 23 January 2023).

[18] Pragya Prasun v Union of India (2025) INSC 599 (SC).

The petitioners included people with disabilities specifically, acid-attack survivors with facial ocular disfigurement, and an individual with 100% visual impairment. They challenged the inaccessibility of digital KYC, e-KYC, video KYC procedures. “liveness” checks that required actions like blinking, facing camera, reading on-screen text etc., which many persons with certain disabilities cannot perform. These procedures are often prerequisites for services like opening bank accounts, obtaining SIM cards, access to welfare schemes etc. Petitioners argued that such inaccessible digital authentication onboarding systems effectively denied them fundamental rights, statutory disability rights, and violated constitutional provisions.

- Main questions:

1. Whether the existing digital KYC, e-KYC, video-KYC, liveness test systems create an unreasonable barrier discrimination for persons with disabilities, and violate their constitutional and statutory rights.
2. Whether these systems must be made accessible in ways that accommodate disabilities (reasonable accommodation, alternate options etc.).
3. What standards directives remedial measures need to be mandated for regulators service providers to ensure inclusivity.

- **The Supreme Court, in a judgment by Justice R. Mahadevan & Justice J.B. Pardiwala, held:**

Right to digital access as integral part of Article 21: The Court recognized that access to digital systems (especially where services, essential functions, identity verification, citizenship, telecom, banking etc. are increasingly mediated digitally) is not a “luxury” but forms a part of the right to life and dignity under Article 21. Excluding or creating barriers for disabled persons in these digital authentication systems infringes on these rights.

1. Statutory obligations under RPWD Act: The Court held that the RPWD Act, 2016 (and its Rules, such as Rule 15) impose binding obligations for accessibility. Systems that impose procedures incompatible with certain disabilities e.g. blinking, eye movement, reading text without alternative reasonable accommodation are discriminatory.
2. Liveness checks digital KYC procedures must allow inclusive alternatives: The Court directed regulators and service providers to modify digital KYC, e-KYC, video-KYC processes so that they are not rigidly requiring actions that some PwDs cannot perform. Alternative methods of “liveness” or no requirement for those movements must be acceptable.

3. Regulators to issue binding guidelines rules to ensure compliance across sectors (banking, telecom, Aadhaar authentication, etc.) with accessible digital identity verification KYC etc., including grievance redress, oversight, periodic audits etc.
4. Declaration of digital inclusion digital accessibility as constitutional duty: The Court emphasized that states regulated entities must proactively ensure accessibility, reasonable accommodation, removing barriers in digital infrastructure.

- Directions / Reliefs Issued

Some of the concrete directions (not exhaustive) include:

1. Regulators such as Reserve Bank of India (RBI), Department of Telecommunications (DoT), SEBI etc. must issue guidelines to ensure digital KYC / video KYC are accessible.
2. Service providers must provide alternative authentication kind of options for persons unable to comply with standard liveness checks for example, alternatives to blinking, or reading text etc.
3. Accessibility compliance – in design, digital platforms, apps etc., must conform to standards such as Web Content Accessibility Guidelines WCAG government prescribed ICT accessibility norms.
4. Grievance redressal mechanism, training of personnel etc. to support persons with disabilities in these digital processes.

- Impact:

1. This is a landmark decision in India's jurisprudence on disability rights in the digital age. It brings digital exclusion squarely within the scope of fundamental rights.
2. The judgment pushes regulators private entities and service providers to rethink how digital identity and verification systems are designed — so as not to impose arbitrary or uniform requirements that exclude those with disabilities.
3. It enforces the concept of *reasonable accommodation* in digital authentication verification processes. Prior to this, there was often an assumption that digital KYC, video KYC was neutral universal, ignoring that many users have disabilities that make standard processes unusable.
4. It aligns Indian law with international norms e.g. UN Convention on the Rights of Persons with Disabilities, which mandates accessibility, etc.

[judgment is significant primarily for issues relating to digital accessibility, disability rights, and inclusive KYC authentication norms.]

1. **RBI v. Sahara India Financial Corporation Ltd.** [19]

- Facts:

1. Sahara India Financial Corporation Ltd. (SIFCL), an NBFC, was under the regulatory oversight of the RBI.
2. RBI found that Sahara had violated KYC guidelines and failed to comply with certain directions issued by it.
3. Based on non-compliance, the RBI issued a direction to Sahara under Section 45MC of the RBI Act, 1934, restricting them from accepting deposits unless they complied with the guidelines.
4. Sahara challenged the RBI's directions in the Allahabad High Court, which ruled in Favor of Sahara.
5. RBI appealed the decision before the Supreme Court.

- Key Issues:

1. Whether the RBI had the authority to issue directions to an NBFC regarding KYC and other compliance matters.
2. Whether Sahara's operations were in violation of the KYC norms and RBI's directions.
3. Whether the High Court was correct in interfering with RBI's regulatory decision.

- **Supreme Court Judgment:**

1. The Supreme Court upheld the RBI's regulatory authority and reversed the High Court's decision.
2. It stated that:

   The Reserve Bank of India it is not just another statutory authority. It is a central bank and has a crucial role in maintaining the financial stability of the country.

- **Key Findings:**

[19] RBI v Sahara India Financial Corporation Ltd (2008) 7 SCC 135.

1. RBI has wide powers under the RBI Act to regulate and supervise NBFCs.
2. KYC norms are an essential part of RBI's regulatory framework to prevent money laundering, financial frauds, and to ensure transparency.
3. The High Court should not interfere in policy regulatory decisions made by a specialized body like the RBI unless there is gross unreasonableness or mala fide.
4. Sahara's failure to comply with KYC requirements was a serious breach, and RBI's action was justified.
5. Significance: Established that financial institutions cannot bypass KYC requirements. Regulatory authorities have full power to penalize and restrict operations in case of non-compliance.

2. **State Bank of India v. Santosh Gupta**[20]

- Facts:

Respondent Santosh Gupta took a housing loan from State Bank of India (SBI) and failed to repay it.

1. SBI initiated recovery proceedings under the SARFAESI Act, 2002 Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act.
2. The respondent challenged these proceedings in the High Court of Jammu & Kashmir, arguing that:

SARFAESI Act could not be enforced in J&K, since land laws like ownership and transfer of immovable property fall under the J&K State's exclusive legislative powers under its special status Article 370 of the Constitution.

The Transfer of Property Act, as applicable in J&K, conflicted with the provisions of the SARFAESI Act.

3. The J&K High Court agreed with this view and held that the SARFAESI Act is not enforceable in the state to the extent it interferes with local laws relating to immovable property.

- Issue:

[20] State Bank of India v Santosh Gupta (2017) 2 SCC 538.

Can KYC norms be diluted in regions with special status laws?

Whether SARFAESI Act Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 is applicable to the State of Jammu & Kashmir and whether the High Court's view that certain sections of SARFAESI were beyond Parliament's legislative power under the constitutional distribution of powers is correct

- Held: The Supreme Court held that KYC is a mandatory national-level requirement, aimed at securing the financial system and preventing misuse. Local laws cannot override central KYC obligations.
- Significance: Reinforced that KYC applies uniformly across India, regardless of special state provisions.

3. **Vijay Madanlal Choudhary v. Union of India**[21]
   - Fact

     The case involved a batch of petitions challenging various provisions of the Prevention of Money Laundering Act, 2002 PMLA.

     The petitioners, including Vijay Madanlal Choudhary, raised concerns about constitutional validity of PMLA provisions, especially those that:
     - Allowed arrest, seizure, and attachment of property without FIR
     - Denied access to the Enforcement Case Information Report (ECIR)
     - Reversed the presumption of innocence
     - Imposed stringent bail conditions under Section 45 of PMLA
   - **Legal Issues**

1. Is the PMLA unconstitutional for violating fundamental rights such as:
   - Article 14 Equality before law
   - Article 20 Protection against self-incrimination
   - Article 21 Right to life and personal liberty

1. Is it valid for the Enforcement Directorate (ED) to:

   Not supply the ECIR to the accused?

   Exercise wide powers of search, seizure, arrest, and attachment without judicial

[21] Vijay Madanlal Choudhary v Union of India (2022) 10 SCC 386.

oversight?

2. Is the twin bail condition under Section 45(1) of the PMLA constitutional?

➢ Supreme Court's Judgment (Major Findings)

1. **PMLA is Constitutionally Valid**[22]

The Court upheld the constitutional validity of the PMLA and its core provisions.

It ruled that money laundering is a serious economic offence affecting national security and integrity.

2. ECIR Need Not Be Furnished to Accused

The ECIR (Enforcement Case Information Report) is not equivalent to an FIR.

Not giving a copy of the ECIR does not violate Article 21, if the grounds of arrest are informed to the accused.

3. ED's Powers Are Not Unconstitutional

The Court ruled that ED is not a police agency, so CrPC norms like Section 154, 161, etc. do not automatically apply.
ED's power of summons, search, seizure, and arrest under the Act is valid and reasonable in the context of money laundering.

4. Twin Bail Conditions Are Valid

The twin conditions under Section 45(1) i.e., public prosecutor must oppose bail, and court must be satisfied that the accused is not guilty and unlikely to commit an offence while on bail were held to be constitutional.
These conditions are necessary due to the gravity of money laundering.

5. Criticism and Later Developments

The judgment was heavily criticized for being ED friendly and weakening procedural safeguards.

In 2023, in a separate case e.g., Manoj Lalwani v. Union of India, the Supreme Court agreed to re-examine parts of this ruling, especially regarding: ECIR non-disclosure Bail conditions

Relevance to KYC / AML (anti–money laundering)

This case is directly relevant to KYC (Know Your Customer) and AML (Anti-Money Laundering) laws:

[22] SEBI v Rose Valley Real Estate & Construction Ltd (Supreme Court of India, 2019).

PMLA is the legal backbone of AML (anti–money laundering) in India. KYC compliance is one of the first defences against money laundering. The judgment- Strengthened the enforcement powers of ED Reaffirmed the importance of compliance with PMLA, including proper customer due diligence Created a precedent that makes non- compliance riskier for financial institutions

4. **SEBI v. Rose Valley Real Estate & Construction Ltd. (2019, SC)**[23]

- Facts

Rose Valley Real Estate & Construction Ltd. had been involved in raising funds from the public through its "Ashirbad" scheme, which was found to be a Collective Investment Scheme (CIS) under the SEBI Act. The company failed to obtain the necessary registration from SEBI to operate such a scheme, leading to regulatory actions.

In June 2014, SEBI directed the company to wind up its scheme and refund the money collected from investors within three months. The company was also required to submit a winding-up and repayment report to SEBI, along with bank account statements indicating refunds to investors and receipts from the investors acknowledging such refunds.

Subsequently, in December 2017, SEBI imposed a penalty of ₹26 crore on Rose Valley Real Estate and its directors for mobilizing funds from investors through illegal money pooling schemes without complying with the regulatory norms.

- **Issues:**

The primary issues in this case revolved around:

1. Non-Compliance with SEBI Regulations: Rose Valley's failure to register its CIS with SEBI, as required under Section 11AA of the SEBI Act, leading to unauthorized fund mobilization.
2. Investor Protection: Ensuring that investors' funds were safeguarded and returned, as the company had collected substantial amounts from the public without regulatory oversight.
3. Regulatory Enforcement: The extent of SEBI's authority and actions in enforcing compliance and penalizing entities violating securities laws

5. **United States v. HSBC Holdings plc (2012, US Federal Court)**[24]

[23] SEBI v Rose Valley Real Estate & Construction Ltd (Supreme Court of India, 2019).
[24] United States v HSBC Holdings plc No 12-CR-763 (E.D.N.Y 2012).

United States v. HSBC Holdings plc & HSBC Bank USA, N.A. Court: U.S. District Court for the Eastern District of New York. Date of DPA: December 11, 2012

Presiding Judge: Hon. John Gleeson

Case Type: Deferred Prosecution Agreement (DPA) involving criminal violations of U.S. anti- money laundering and sanctions laws.

- FACTS:

1. Massive Money Laundering by Drug Cartels

HSBC Mexico (an affiliate of HSBC Group) moved $7 billion in U.S. dollars into the U.S. banking system from 2007 to 2008. The funds were suspected to be proceeds from Mexican and Colombian drug trafficking organizations, including the Sinaloa Cartel.

2. Failure of KYC

HSBC USA failed to:

Conduct proper customer due diligence on high-risk foreign affiliates and clients.
Monitor suspicious transactions.
File required Suspicious Activity Reports (SARs) under the Bank Secrecy Act (BSA).
Foreign correspondent accounts — particularly those in Mexico, the Cayman Islands, and the Middle East — were not properly vetted or risk-assessed.

3. Sanctions Violations

HSBC processed over $660 million in transactions involving sanctioned countries Iran, Sudan, Cuba, Burma, and Libya. It used "stripping" techniques — deliberately removing identifying information from payment instructions — to avoid detection by U.S. regulators.

4. Internal Warnings Ignored

HSBC's compliance staff repeatedly raised red flags, but executives and business units overrode or ignored recommendations to close suspicious accounts. A 2002 internal audit already labelled HSBC Mexico’s controls as a "major risk", but action was delayed.

- LEGAL ISSUES

1. Did HSBC violate U.S. KYC and AML (anti–money laundering) regulations under the Bank Secrecy Act (BSA)?

Yes. HSBC wilfully failed to implement an effective AML (anti–money laundering) program and ignored its obligations to perform KYC on high-risk customers and foreign affiliates.

2. Was HSBC liable for failing to perform due diligence on foreign correspondent accounts?

Yes. U.S. law requires banks to conduct enhanced due diligence on foreign correspondent banking relationships under the Patriot Act and BSA. HSBC failed to meet this duty.

3. Were HSBC's compliance failures sufficient to warrant criminal charges?

Yes. The Department of Justice (DOJ) filed criminal information (not a full indictment) with charges of:

Wilful failure to maintain an AML (anti–money laundering) program

Failure to conduct due diligence on correspondent accounts Violations of U.S. sanctions laws (e.g., International Emergency Economic Powers Act (IEEPA))

4. Could the Court review or reject the terms of the DPA?

No. The court expressed concern over the seriousness of HSBC's misconduct but ultimately had limited authority to revise or reject the Deferred Prosecution Agreement, as ruled later by the 2nd Circuit Court of Appeals.

- Held: HSBC admitted wrongdoing and entered a $1.9 billion settlement with US authorities under the Bank Secrecy Act and Patriot Act.

- Significance: Demonstrated that non-compliance with KYC is not only a regulatory breach but can lead to criminal prosecution and huge financial penalties.

[judgment is significant primarily for or several doctrines and developments in U.S. financial, criminal, regulatory law. Below is an outline of what the case is about, and what legal principles, lessons it illustrates]

6. **FinCEN v. Ripple Labs Inc. (2015, US)[25]**

- Facts:

1. FinCEN: U.S. agency that enforces the Bank Secrecy Act (BSA), which governs anti-money laundering (AML) obligations. Ripple Labs Inc.: A U.S.-based company that created and operates the Ripple payment protocol and associated cryptocurrency XRP.
2. Ripple developed and sold a virtual currency (XRP), and operated as a money services business (MSB) by engaging in the sale and transfer of XRP. Ripple failed to register with FinCEN as a money services business as required under U.S. law. Ripple also failed to implement and maintain an effective Anti-Money Laundering (AML) program.
3. Between 2013 and 2015, Ripple Labs and its subsidiary XRP II, LLC conducted virtual currency transactions without registering or complying with AML (anti–money laundering) rules. Ripple agreed to a civil money penalty of $700,000 and to take remedial steps, including:
    - Registering as an MSB
    - Implementing a robust AML (anti–money laundering) compliance program
    - Enhancing internal controls and audits
    - Conducting regular training and independent reviews
    - Cooperating with future investigations
4. This was the first civil enforcement action by FinCEN against a virtual currency exchanger. It was brought in coordination with the U.S. Department of Justice (DOJ) and resolved via non-prosecution agreement.

- LEGAL ISSUES

[25] FinCEN v Ripple Labs Inc (2015) Case No 2015-05.

1. Whether Virtual Currency Businesses Are "Money Transmitters" Under the BSA

FinCEN determined that Ripple was acting as a “money transmitter,” and thus required to register and comply with AML (anti–money laundering) laws. This established that virtual currency exchangers and administrators are not exempt from BSA obligations even if the digital asset is not considered legal tender.

2. Failure to Implement an Effective AML (anti–money laundering) Program

Ripple had no written AML (anti–money laundering) procedures during the relevant period.
It failed to verify the identity of its customers or monitor transactions for suspicious activity.

3. FinCEN’s Authority Over the Crypto Sector

The case confirmed that FinCEN has enforcement jurisdiction over virtual currencies, even in the absence of comprehensive cryptocurrency legislation at the time.
Ripple was subject to regulatory obligations under existing laws (BSA), despite operating in a "new" technology space.

4. The Role of Civil Settlements and Non-Prosecution Agreements in Crypto Regulation

The Ripple case was resolved through a settlement and a non-prosecution agreement, rather than a full criminal or civil trial.
This strategy avoided lengthy litigation while still achieving regulatory compliance and public accountability.

- **Significance / Impact**[26]

1. First federal enforcement action against a cryptocurrency company for AML (anti–money laundering) violations.
2. Confirmed that virtual currency businesses must comply with Bank Secrecy Act obligations.
3. Highlighted the growing regulatory scrutiny of the crypto sector by U.S. agencies.
4. Ripple’s early regulatory trouble helped shape how crypto firms approached compliance in the U.S. going forward.

26

[Judgment is significant primarily for the domains of financial regulation, anti-money laundering (AML), and cryptocurrency law, and it continues to influence regulatory compliance frameworks for virtual asset businesses worldwide.]

7. **R v. NatWest Bank Plc (2021, UK Crown Court)[27]**

➢ Facts of the Case

1. NatWest was prosecuted by the Financial Conduct Authority (FCA) under the Money Laundering Regulations 2007 (“MLR 2007”). This was the first criminal prosecution by the FCA under those Regulations.
2. Time-frame: The failures occurred between 2012 and 2016 in relation to the accounts of a UK-incorporated customer, *Fowler Oldfield*, a jewellery business.
3. Amounts involved: Over the five-year relationship, approximately £365 million was deposited with NatWest by Fowler Oldfield, of which about £264 million was in cash.
4. Several suspicious indicators (“red flags”) were noted by staff: large cash deposits, Scottish banknotes (outside the locality), cash smelling musty, people depositing large amounts in branches, etc. However, many of these were not acted upon properly.
5. Technical/systems failures:

   The bank’s automated monitoring treated some cash deposits as cheque deposits — thereby underestimating risk.
   Insufficient ongoing monitoring of the business relationship, and inadequate risk-sensitive reviews.
6. Pleas & conviction: NatWest pleaded guilty in October 2021 to three offences under *Regulation 45(1) of the MLR 2007*, which encompassed failures to comply with certain parts of regulations 8(1), 8(3), 14(1) in respect of conducting ongoing monitoring, risk-sensitive monitoring, and enhanced monitoring in situations of higher risk.
7. Sentence: On 13 December 2021 at Southwark Crown Court, NatWest was fined £264,772,619.95, ordered to pay £4,297,466 in costs, and a confiscation order of approximately £460,000 was made.

➢ **Legal Issues**

[27] R v NatWest Bank Plc (Southwark Crown Court, 13 December 2021).

1. Obligations under MLR 2007

Regulation 8(1): ongoing monitoring of business relationships.

Regulation 8(3): determining the extent of monitoring in a risk-sensitive manner and being able to demonstrate it to supervisory authority.
Regulation 14(1): enhanced ongoing monitoring where risk is higher.

2. **Systemic and operational failures**

Failure to act on internal warnings / red flags.

Weakness in automated systems (misclassification of cash deposits etc.).
Lack of periodic review and risk reassessment.

3. **Strict liability offences under MLR 2007**

The breach does not require proof of intentional wrongdoing or complicity in money laundering itself. The bank could be convicted even where it did not knowingly assist criminality, but simply failed in its statutory obligations.

4. **Corporate liability and regulatory enforcement**

The case shows regulation can hold large financial institutions criminally liable for failures of compliance systems, even if individuals are not charged.
The role of FCA as an enforcement authority, exercising criminal powers under MLR 2007.

- **Significance**

1. Precedent: First time a major bank in the UK was criminally prosecuted under the Money Laundering Regulations for compliance failures. Signals that such statutory/regulatory obligations are enforceable criminally, not just regulatory/civil.

2. Scope of regulatory obligations: The case clarifies what "ongoing monitoring", "risk-sensitive monitoring," and "enhanced monitoring" mean in practice, particularly considering changing customer behaviour or business models. It shows banks must be alert not just to what customers do at onboarding, but over the lifecycle of the relationship.
3. Systemic importance of compliance systems: Demonstrates that failure in internal systems (automated transaction monitoring, staff escalation, risk profiling) can lead to very large penalties.
4. Deterrent effect: The size of the fine (over £260 million) underscores the financial stakes of

non-compliance. For banks and other regulated entities, this case sends a strong message that compliance must be actively managed, resourced, and audited.

5. Regulatory enforcement posture: Reflects how regulators like the FCA are increasingly willing to use criminal powers for non-intentional but serious compliance failures. Also shows early guilty pleas receive significant discounts.
6. Comparative regulatory law: Useful in comparative studies, especially for legal frameworks involving AML/CTF (anti–money laundering counter-terror financing), the strictness of liability, and obligations of financial institutions.

SUGGESTIONS & CONCLUSION:

Promote secure video-KYC, AI-based verification, and biometric integration & develop multilingual digital platforms to reduce exclusion in rural areas. Adopt strict data retention and confidentiality protocols. Enforce accountability for breaches under the Data Protection Act and IT framework. Standardize KYC norms for banks, NBFCs, fintech apps, cryptocurrency exchanges, and payment wallets. Create a centralized KYC registry accessible to authorized agencies. Conduct training for employees of banks, digital platforms, and cooperative institutions. Educate customers on documentation, updating, and fraud prevention. Introduce risk-based KYC renewal instead of uniform deadlines. Use transaction analytics to monitor suspicious behavior. Simplify KYC for low-income groups with alternative ID options. Leverage Aadhaar-based e-KYC only with consent and privacy safeguards. Penalize non-compliance by institutions and intermediaries. Create cross-agency coordination between FIU, RBI, and law enforcement. Align Indian KYC norms with FATF recommendations and OECD guidelines. Encourage mutual recognition frameworks for cross-border financial transactions.

The Know Your Customer (KYC) process has become an indispensable tool in today's financial and regulatory environment. It safeguards the integrity of financial systems by preventing money laundering, terrorist financing, fraud, and other financial crimes. KYC not only ensures regulatory compliance but also strengthens transparency, accountability, and trust between institutions and their customers. By verifying identity and assessing risks, it promotes secure transactions and protects customers from misuse of their financial profiles. Thus, the need for KYC is not merely a legal obligation but a global best practice essential for sustainable, ethical, and secure financial operations.

References

- Navi Technologies, 'KYC Full Form' (Navi, 2025) https://navi.com/blog/kyc-full-form/ accessed 10 January 2025.

- Akhilesh S Dubey, *Treatise on Prevention of Money Laundering Act, 2002* (2nd edn, 2025).

- KYC AML Guide, 'Risk Management in KYC' (KYC AML Guide, 2025) https://kycaml.guide/blog/risk-management-in-kyc/ accessed 10 January 2025.

- Gagandeep Singh, *The KYC Handbook: Mastering Customer Due Diligence* (7 July 2025).

- Persona Identities Inc, 'KYC Best Practices for Global Compliance' (Persona Blog, 2025) https://withpersona.com/blog/kyc-best-practices-for-global-compliance accessed 10 January 2025.

- Barclays India, 'Importance of KYC' (Barclays) https://www.barclays.in/content/dam/barclays-in/documents/download-forms/kyc/Importance_of_KYC.pdf accessed 9 January 2025.

- Benjamin Vogel and Jean-Baptiste Maillart, *National and International Anti-Money Laundering Law* (2024).

- R Rajagopal v State Bank of India (Madras HC, 2019).

- KYC Hub, 'Global KYC Regulations: Key Requirements and Compliance' (KYC Hub, 2024) https://www.kychub.com/blog/global-kyc-regulations/ accessed 9 January 2025.

- 'Danske Bank Case: Money Laundering Scandal' (Sanction Scanner, 2023) https://www.sanctionscanner.com/blog/danske-bank-case-money-laundering-scandal-11302 accessed 10 January 2025.

- Infosys BPM, 'Key Components of KYC' (Infosys BPM, 2024) https://www.infosysbpm.com/blogs/financial-services/key-components-of-kyc.html accessed 9 January 2025.

- Shubham Sharma, 'The Future of KYC: Top KYC Trends in 2025' (KYC Trends, 2025) https://kyctrends.com/future-kyc-2025 accessed 10 January 2025.

- Justice KS Puttaswamy (Retd) v Union of India (2018) 10 SCC 1.

- Binoy Viswam v Union of India (2017) 7 SCC 59.

- Lokniti Foundation v Union of India BS827420 (SC 2016).

- Shanta Sinha v Union of India, Writ Petition (Civil) No 342 of 2017.

- Government of India, 'KYC Awareness Document' (Ministry of Finance, 2023) https://cdnbbsr.s3waas.gov.in/... accessed 9 January 2025.

- Persona, 'KYC in Banking' (2024) https://withpersona.com/blog/kyc-in-banking accessed 10 January 2025.

- Indian Institute of Banking and Finance, 'Anti-Money Laundering and KYC' (IIBF, 23 January 2023).

- Pragya Prasun v Union of India (2025) INSC 599 (SC).

- RBI v Sahara India Financial Corporation Ltd (2008) 7 SCC 135.

- State Bank of India v Santosh Gupta (2017) 2 SCC 538.

- Vijay Madanlal Choudhary v Union of India (2022) 10 SCC 386.

- SEBI v Rose Valley Real Estate & Construction Ltd (Supreme Court of India, 2019).
- United States v HSBC Holdings plc No 12-CR-763 (E.D.N.Y 2012).
- FinCEN v Ripple Labs Inc (2015) Case No 2015-05.
- R v NatWest Bank Plc (Southwark Crown Court, 13 December 2021).
- Indian Kanoon, 'KYC Case Law Search' https://indiankanoon.org/search/?formInput=kyc%20 accessed 9 January 2025.
- Economic Law Practice, 'Analysis of RBI Norms on KYC Data Privacy' (ELP Law, 2024) https://elplaw.in/... accessed 9 January 2025.
- Taxmann, 'Director KYC Non-Compliance: Expert Opinion' (Taxmann, 2024) https://www.taxmann.com/... accessed 9 January 2025.