

Analysis of RBI Norms on KYC, Data Privacy, and Confidentiality Obligations in Banking

The Importance of KYC Norms and Data Privacy in Banking

In today's globalized and digital economy, safeguarding financial systems from illicit activities like money laundering, terrorist financing, and fraud is paramount. At the core of this effort lie robust Know Your Customer (KYC) norms and data privacy frameworks, ensuring that banks and financial institutions can identify and verify their customers while maintaining the confidentiality of sensitive information. The Reserve Bank of India (RBI), through its Master Directions on KYC, has established a comprehensive framework to address evolving challenges in the financial sector. This update explores the historical evolution of KYC norms, their significance in combating financial crimes, the obligations of banks and customers, and the legal frameworks ensuring data privacy. It also examines the implications of global regulations and judicial precedents in shaping the banking sector's compliance and confidentiality obligations.

Background and Historical Perspective

The framework of Know Your Customer (KYC) norms and data privacy in banking has evolved globally to combat financial crimes like money laundering, terrorist financing, and fraud. In India, these norms derive their foundation from international standards set by the **Financial Action Task Force (FATF)** and domestic laws like the **Prevention of Money Laundering Act (PMLA), 2002**.

Historical Evolution:

- **Pre-2000:** Indian banking operated with limited regulation on customer verification. The concept of customer due diligence (CDD) was rudimentary, focusing only on basic account opening documentation.
- **Post-2002:** With the enactment of PMLA and FATF membership, India strengthened its anti-money laundering (AML) and countering terrorist financing (CFT) mechanisms. RBI introduced its first formal KYC guidelines.
- **2016 KYC Directions:** RBI consolidated KYC guidelines into a comprehensive framework through its **Master Direction on KYC, 2016¹**, outlining customer identification, monitoring, and reporting obligations.
- **2024 Amendments:** The RBI updated KYC norms in 2024 to enhance compliance, integrate advanced technology, and strengthen data privacy protections.

Banks are required to carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. Banks are also required to ensure overall compliance with the obligations imposed under PML Act and the Rules and nominate a Designated Director and a Principal Officer who shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the LA/regulations.

No Banks can carry out transaction or account-based relationship without following the CDD procedure. Banks are also required to :

- maintain all necessary records of transactions between the RE and the customer, both domestic and international, for at least five years from the date of transaction;
- preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;

¹ <https://www.rbi.org.in/commonman/English/scripts/notification.aspx?id=2607>

- make available swiftly, the identification records and transaction data to the competent authorities upon request;
- introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
- maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
 - the nature of the transactions;
 - the amount of the transaction and the currency in which it was denominated;
 - the date on which the transaction was conducted; and the parties to the transaction.

Significance of RBI KYC Norms

The 'Know Your Customer' guidelines were issued by the RBI in February 2005 revisiting the earlier guidelines issued in January 2004 in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT). These standards have become the international benchmark for framing Anti Money Laundering and combating financing of terrorism policies by the regulatory authorities. Compliance with these standards by the banks/financial institutions/NBFCs in the country have become necessary for international financial relationships.

The KYC norms issued by the RBI serve as the backbone of secure and transparent banking operations. These norms ensure:

- **Prevention of Financial Crimes:** Verification of customer identity deters money laundering, fraud, and terrorism financing.
- **Financial Stability:** Accurate customer profiling mitigates risks to the financial system.
- **Global Compliance:** Aligning Indian banking practices with FATF standards fosters trust in international markets.
- **Consumer Protection:** Protecting customers from identity theft and fraud by establishing robust verification mechanisms.

Customer Due Diligence (CDD) in RBI KYC Guidelines

Customer Due Diligence (CDD) is a critical process outlined in the **Reserve Bank of India's (RBI) Master Direction on KYC** guidelines. It involves verifying the identity of customers, beneficial owners, and entities to prevent money laundering, terrorist financing, and other illicit activities. CDD is essential for maintaining the integrity of financial institutions and ensuring compliance with the **Prevention of Money Laundering Act (PMLA), 2002** and related rules.

Key Components of CDD

CDD requires financial institutions to collect, verify, and maintain customer data at various stages of their engagement. Below are the main components of CDD as per the RBI guidelines:

- **Identification and Verification**
 - **For Individuals:**
 - Submission of Aadhaar (with consent) or other **Officially Valid Documents (OVDs)** such as a passport, voter ID, or driving license.
 - Verification of the customer's identity using reliable and independent sources.
 - Cross-verification of PAN or Form 60 for accounts requiring tax identification.
 - **For Non-Individuals:**
 - Identification of beneficial owners (natural persons who own or control more than 10% of a company's equity or assets).
 - Verification of authorized signatories and persons acting on behalf of the legal entity.
- **Risk-Based Approach**
 - Customers are categorized into **low, medium, and high-risk** categories based on their profile, geographical location, type of business, and transaction patterns.
 - Enhanced due diligence (EDD) is applied to high-risk customers, requiring deeper verification and monitoring.

- **Ongoing Due Diligence**
 - Monitoring transactions to ensure they align with the customer's declared financial activities.
 - Identifying and investigating unusual or suspicious transactions.
 - Periodically updating KYC records, including addresses and contact information.
- **Simplified Due Diligence**
 - Allowed for "small accounts" with limited features, such as:
 - Account balance capped at ₹50,000.
 - Annual credits not exceeding ₹1,00,000.
 - KYC requirements are relaxed, but with strict monitoring.
- **Enhanced Due Diligence (EDD)**

EDD is mandatory for:

- High-risk customers or accounts.
- Cross-border transactions.
- Customers from jurisdictions with inadequate AML/CFT standards.

When is CDD Required?

CDD must be conducted in the following situations:

- **Opening an Account:** At the commencement of a financial relationship with a customer.
- **Occasional Transactions:** For transactions amounting to ₹50,000 or more, whether conducted as a single or multiple connected transactions.
- **Suspicious Activity:** When there is doubt about the authenticity or adequacy of previously collected customer identification data.
- **Periodic Updates:** As part of the bank's ongoing KYC compliance procedures.

Obligations for Banks Under CDD

- **Data Collection and Verification:**
 - Banks must verify the authenticity of customer-provided documents. They should rely on reliable third-party data (such as Central KYC Records Registry - CKYCR) wherever possible.
- **Periodic Reviews:**
 - Banks must update customer data periodically and align it with changing risk profiles.
- **Reporting Suspicious Transactions:**
 - Transactions that appear unusual, complex, or inconsistent with a customer's profile must be reported to the **Financial Intelligence Unit - India (FIU-IND)**.

Changes Introduced in 2024

- **Key Changes in RBI Master Direction on KYC (2024)**
 - **Enhanced V-CIP:** Strengthened facial recognition, GPS tagging, timestamping, and mandatory encryption for secure video-based verification.
 - **Data Localization:** Customer data, including V-CIP recordings, must be stored in India, with cloud solutions allowed only if the bank retains full control.
 - **Simplified KYC for Small Accounts:** Relaxed documentation requirements with strict transaction limits and simplified updates for low-risk customers.
 - **CKYCR Integration:** Mandatory retrieval and regular updating of KYC records from the Central KYC Records Registry to minimize duplication.

- **High-Risk Monitoring:** Intensified due diligence and periodic verification for high-risk customer profiles.
- **Periodic Updates:** Clear timelines for updating KYC based on the customer's risk profile.
- **Digital KYC:** Stricter security for Aadhaar-based processes and mandatory digital authentication for online submissions.

These updates are aimed at enhancing compliance, customer security, and operational efficiency in the financial sector.

International Obligations and Reporting Requirements under the RBI Master Directions

The KYC guidelines emphasise on:

- **Daily Monitoring of Sanctions Lists:** Lists from UNSC, UAPA, and WMD Act must be verified daily to ensure up-to-date compliance.
- **Reporting Obligations:** Matches in sanctions lists must be reported to relevant authorities like FIU-IND, CNO, and the MHA.
- **Enhanced Due Diligence:** FATF high-risk jurisdictions require stringent checks and documentation.
- **Confidentiality and Privacy:** REs must maintain customer confidentiality except in cases of legal compulsion or public interest.

The evolution of KYC norms reflects the growing importance of secure banking systems in a digital era. However, practical implication of International Obligations for Indian Banks are significant.

Key International Obligations and Their Implications

- **FATF Recommendations:** Indian banks must implement risk-based AML/CFT programs and conduct enhanced due diligence (EDD) for high-risk customers and jurisdictions. Compliance ensures access to global financial systems but involves significant costs and challenges, such as integrating cross-border data-sharing protocols with local privacy laws.
- **UNSC Resolutions:** Banks must also monitor daily and update databases with sanctions lists (e.g., ISIL, Al-Qaeda, Taliban, North Korea). Transactions involving flagged entities require immediate reporting, though real-time updates can strain smaller banks and disrupt legitimate transactions due to false positives.
- **UAPA, 1967²:** Banks must freeze assets of listed entities without prior notice and conduct thorough checks during onboarding and audits. This can lead to disputes with customers and requires extensive staff training for timely compliance.
- **WMD Act, 2005³:** Banks are required to verify customer data against WMD Act lists during onboarding and periodically, with non-compliance leading to penalties and reputational risks.
- **FATCA⁴ and CRS Reporting⁵:** Reporting Financial Institutions must collect and report customer data, including tax residency, to the Income Tax Department. Challenges include data synchronization and ensuring accuracy in self-declaration forms.

² The **Unlawful Activities (Prevention) Act, 1967 (UAPA)** is a comprehensive anti-terror law in India designed to prevent unlawful activities that threaten the sovereignty, integrity, and security of the nation. The Act has significant implications for banks and financial institutions (Regulated Entities, or REs), requiring their active participation in identifying, reporting, and restricting financial transactions linked to terrorist activities.

³ The **Weapons of Mass Destruction and Their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act)** was enacted to prohibit activities related to the proliferation of weapons of mass destruction and their delivery systems. The Act aligns with India's international obligations under treaties such as the **United Nations Security Council Resolutions (UNSCR)** and other global conventions to combat the proliferation of WMDs. Banks and financial institutions (Regulated Entities, or REs) are integral to enforcing compliance with the provisions of this Act.

⁴ The **Foreign Account Tax Compliance Act (FATCA)** is a United States federal law enacted in 2010 to combat tax evasion by U.S. taxpayers holding financial assets and accounts abroad. Indian banks and financial institutions (designated as Reporting Financial Institutions) are required to comply with FATCA under an **Inter-Governmental Agreement (IGA)** signed between India and the U.S.

⁵ The **Common Reporting Standard (CRS)**, developed by the **Organisation for Economic Co-operation and Development (OECD)**, is a global framework for the automatic exchange of financial account information between participating countries to prevent tax evasion. Indian financial institutions, including banks, are required to comply with CRS under the Income Tax Act and associated rules.

- **Basel AML/CFT Standards⁶:** Banks must maintain strong governance, transaction monitoring, and risk management systems, with regular stress testing and reporting to RBI.

Technology Adoption: To meet such challenges the Banks like **HDFC⁷, ICICI and Standard Chartered Bank⁸** have started use of AI tools for real-time monitoring of suspicious transactions. **State Bank of India is also reported to have** partnered with international regulators to align AML/CFT frameworks with global standards. Smaller banks leverage shared resources like the **CKYCR** to reduce compliance costs. Indian Bank Association has also taken initiatives in that regard.

Data Privacy and Confidentiality Obligations in Banking

The banking sector operates at the nexus of trust and confidentiality, where safeguarding customer data is paramount. Financial institutions, while collecting and maintaining sensitive customer information, face dual obligations: ensuring data privacy and complying with disclosure requirements under the law. The legal framework for data privacy and confidentiality in India is anchored in various statutes, with significant emphasis on balancing customer protection and lawful disclosures.

Legal Framework: Key Statutory Provisions

- **State Bank of India Act, 1955**
 - **Section 44⁹:** Recognizes the importance of maintaining customer confidentiality specific to SBI. It allows disclosures only under legally sanctioned circumstances or when it serves the public interest, balancing privacy with national priorities.
- **Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970/1980**
 - **Section 13¹⁰:** This section extends confidentiality obligations to public sector banks. Disclosures of customer information are permitted only when directed by legal authorities, ensuring compliance without breaching trust.
- **Information Technology Act, 2000**
 - **Section 43A:** Imposes liability on banks for failing to protect sensitive personal data. This provision mandates robust data protection measures and holds banks accountable for negligence in data security.
 - **Section 72A:** Criminalizes unauthorized disclosure of customer data, ensuring strict penalties for breaches by employees or third-party service providers.

⁶ The **Basel Committee on Banking Supervision (BCBS)** issues Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) standards as part of its global regulatory framework. These standards provide guidelines for managing financial risks, ensuring proper governance, and maintaining financial system integrity. Indian banks, regulated by the **Reserve Bank of India (RBI)**, align with Basel AML/CFT standards to strengthen their risk management frameworks.

⁷ <https://www.hdfcbank.com/personal/about-us/news-room/press-release/2023/q1/hdfc-bank-partners-with-microsoft-as-part-of-its-digital-transformation-journey>

⁸ <https://economictimes.indiatimes.com/wealth/save/a-new-weapon-against-online-payment-frauds-timely-alerts-on-transactions-via-upi-debit-card-credit-card-net-and-mobile-banking/articleshow/110484847.cms?from=mdr>

⁹ **44. Obligation as to fidelity and secrecy.** The State Bank shall observe, except as otherwise required by law, the practices and usages customary among bankers and, in particular, it shall not divulge any information relating to or to the affairs of its constituents except in circumstances in which it is, in accordance with the law or practice and usage customary among bankers, necessary or appropriate for the State Bank to divulge such information. (2) Every director, member of a Local Board or of a Local Committee, auditor, adviser, officer or other employee of the State Bank shall, before entering upon his duties, make a declaration of fidelity and secrecy as in the form set out in the Second Schedule. (3) Nothing contained in this section shall apply to the credit information disclosed under the Credit Information Companies (Regulation) Act, 2005.

¹⁰ **13. Obligations as to fidelity and secrecy.**—(1) Every corresponding new bank shall observe, except as otherwise required by law, the practices and usages customary among bankers, and, in particular, it shall not divulge any information relating to or to the affairs of its constituents except in circumstances in which it is, in accordance with law or practices and usages customary among bankers, necessary or appropriate for the corresponding new bank to divulge such information.

(2) Every director, member of a local board or a committee, or auditor, adviser, officer or other employee of a corresponding new bank shall, before entering upon his duties, make a declaration of fidelity and secrecy in the form set out in the Third Schedule. (3) Every Custodian of a corresponding new bank shall, as soon as possible, make a declaration of fidelity and secrecy in the form set out in the Third Schedule. (4) Nothing contained in this section shall apply to the credit information disclosed under the Credit Information Companies (Regulation) Act, 2005 (30 of 2005)

- **Credit Information Companies (Regulation) Act, 2005 (CIC Act):**
 - **Section 29:** This section mandates that credit information provided to Credit Information Companies (CICs) by banks and financial institutions must be handled with strict confidentiality. Banks are obligated to ensure that this information is not misused or disclosed to unauthorized parties. Non-compliance can attract penalties under the CIC Act.
- **The Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983 is an act that establishes obligations of fidelity and secrecy for public financial institutions in India (PFI Act):**
 - **Section 3:** This section requires public financial institutions to act in accordance with stringent standards of confidentiality when handling sensitive customer data. It reinforces the responsibility of financial institutions to safeguard data privacy as part of their statutory duties.
- **Payment and Settlement Systems Act, 2007 (PSS Act):**
 - **Section 22:** This section explicitly prohibits payment system providers (such as those managing NEFT, RTGS, etc.) from disclosing the existence or contents of any document or information shared by a system participant (customer). It ensures that sensitive financial transaction data is protected during online payment and settlement processes.

Regulatory Guidelines and Cybersecurity Requirements

- **RBI's "Guidelines on Cyber Security Framework in Banks" (2016)¹¹:**

These guidelines mandate banks to implement measures for preserving the confidentiality, integrity, and availability of customer information. Specific requirements include:

- Encryption of sensitive personal data.
- Controlled access to customer data for authorized personnel only.
- Periodic audits to assess vulnerabilities and ensure compliance.

- **Sensitive Personal Data or Information (SPDI) Rules (Under IT Act, 2000):**

The **SPDI Rules** impose the following obligations:

- **Consent for Collection:** Banks must obtain explicit consent from customers before collecting sensitive data.
- **Lawful Purpose:** Data can only be collected and retained for purposes directly related to the bank's functions.
- **Restriction on Retention:** Once the purpose is served, the data must be securely deleted or anonymized.
- **Restricted Transfer:** SPDI can only be transferred with the customer's consent and for lawful purposes necessary for contract fulfillment.
- **Circumstances Allowing Disclosure:** Banks can disclose customer information in specific situations:
 - **Legal Orders:** Court directives or enforcement of laws (e.g., Income Tax Act, 1961; PMLA, 2002).
 - **Regulatory Requirements:** Reporting to RBI, FIU-IND, or other regulators.
 - **Public Interest:** When disclosure serves public safety or national security.
 - **Customer Consent:** Explicit authorization by the customer.
- **Judicial Precedents privacy as a fundamental right and limited data-sharing to cases meeting legality:**
 - **Govind v. State of Madhya Pradesh (1975)¹²:** Recognized privacy as a constitutional right, emphasizing proportionality in disclosures.
 - **Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)¹³:** Affirmed privacy as a fundamental right and limited data-sharing to cases meeting legality, necessity, and proportionality. The nine Judge Bench unanimously reaffirmed the right to privacy as a fundamental right under the Constitution of India. The Court held that the right to privacy was

¹¹ <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF>

¹² Govind vs State Of Madhya Pradesh & Anr on 18 March, 1975

¹³ Justice K.S. Puttaswamy(Retd) vs Union Of India on 26 September, 2018

integral to freedoms guaranteed across fundamental rights, and was an intrinsic aspect of dignity, autonomy and liberty.

Balancing Compliance and Confidentiality

With the rapid digitization of banking operations, banks face the dual challenge of ensuring compliance with stringent regulations while safeguarding customer privacy. This balance is particularly complex due to evolving global standards, the rise in sophisticated cyber threats, and the operational complexities of implementing advanced technologies. Below are the key challenges and examples illustrating how banks are addressing them:

- **Challenges in Adopting Advanced Technology:**
 - **Integration Costs:** Implementing advanced encryption, AI-driven fraud detection, and real-time monitoring systems can be financially and operationally demanding, especially for smaller banks.
 - **Legacy Systems:** Many banks operate on outdated IT infrastructure, making the integration of modern cybersecurity frameworks complex and time-consuming.
 - **Data Localization Requirements:** Regulations such as mandatory storage of customer data in India (RBI Master Direction 2024) necessitate significant investments in local data centers.
 - **Skilled Workforce:** Ensuring compliance requires a skilled workforce capable of managing cutting-edge technology and understanding global norms.
- **Compliance with Global Norms:**
 - **FATF Recommendations:** Aligning with FATF's AML/CFT standards often requires banks to overhaul their risk assessment processes and monitoring systems.
 - **Cross-Border Operations:** Multinational banks face complexities in reconciling diverse regulatory requirements across jurisdictions, especially for data sharing and privacy norms.
 - **Sanctions Compliance:** Daily updates and monitoring of sanctions lists under UAPA, WMD Act, and UNSC resolutions pose operational challenges due to the volume and frequency of changes.

Growing challenges of Regulatory Compliances and Customer Privacy

To address the growing challenges of regulatory compliance and customer privacy, banks must strike a delicate balance between adhering to stringent norms and safeguarding sensitive customer information. This balance is increasingly complex due to heightened regulatory scrutiny, evolving privacy laws, and the rising threat of cyberattacks. To address these challenges, banks are leveraging advanced technologies like end-to-end encryption, AI-driven threat detection, and multi-factor authentication. However, lapses in compliance can lead to severe regulatory penalties, legal consequences, and erosion of customer trust.

Instances of penalties imposed by the RBI for KYC violations and court rulings on privacy breaches illustrate the gravity of these issues. Additionally, international precedents highlight the global implications of non-compliance. In response, leading banks such as HDFC Bank, SBI, and Yes Bank have embraced innovative technologies to strengthen compliance and customer security. Below are some notable examples of compliance challenges and initiatives undertaken to address them.

Below are some of the notable instances where banks faced penalties for such violations:

- **Reserve Bank of India (RBI) Penalties for KYC Violations**
 - **RBL Bank Ltd. (November 2024):** The RBI imposed a penalty of ₹61.40 lakh on RBL Bank for non-compliance with KYC directives¹⁴. Inspections revealed failures in adhering to prescribed KYC procedures.
 - **Multiple Banks (July 2016):** The RBI penalized 13 banks, including Allahabad Bank, Bank of Baroda, and Canara Bank, for violating KYC norms¹⁵. Penalties ranged from ₹10 million to ₹50 million, depending on the severity of non-compliance.

¹⁴ <https://www.moneylife.in/article/rbi-slaps-rs6140-lakh-penalty-on-rbl-bank-for-not-complying-with-kyc-rules/75701.html>

¹⁵ <https://www.rbi.org.in/commonman/english/Scripts/PressReleases.aspx?id=1822>

▪ Legal Actions Pertaining to Data Privacy Breaches

- **Supreme Court Notice to Credit Information Companies (May 2024)**¹⁶: The Supreme Court issued notices in response to allegations of privacy violations by credit information companies. The plea sought directives to ensure compliance with the Credit Information Companies (Regulation) Act, 2005, aiming to safeguard citizens' privacy rights.
- **Jaiprakash Kulkarni Case (July 2024)**¹⁷: In this case, the court emphasized the importance of banks adhering to RBI's Customer Protection guidelines, especially concerning unauthorized electronic banking transactions. The court highlighted that banks must compensate customers for losses due to third-party fraud, provided the customer promptly reported the fraud and was not negligent.
- **International Precedents: Canara Bank UK entity was Fined in the UK (June 2018)**: The UK's Financial Conduct Authority fined the UK division of Canara Bank £890,000 for systematic anti-money laundering failures, highlighting the global importance of adhering to KYC norms¹⁸.

These instances underscore the critical importance for banks to comply with KYC norms and uphold customer data privacy. Non-compliance not only attracts regulatory penalties but also erodes customer trust and can lead to significant legal challenges. In view of the above challenges, the leading banks, such as **HDFC Bank**, **State Bank of India (SBI)**, and **Yes Bank**, are reported to have embraced advanced technologies to strengthen compliance and customer security:

- **AI-based fraud detection systems** are commonly used to identify suspicious transactions in real-time, enhancing anti-money laundering (AML) measures.
- **Blockchain technology** has been deployed by major banks to maintain secure and tamper-proof transaction records, particularly for high-value operations.
- Robust encryption and **multi-factor authentication** have been implemented across mobile and online banking platforms to prevent unauthorized access and ensure customer data security.

Prominent banks, including **ICICI Bank** and **Canara Bank**, have taken significant steps to address regulatory and operational challenges by transitioning to **centralized data storage systems** to meet data localization requirements while maintaining efficient cross-border operations. Strengthening KYC and AML frameworks after regulatory penalties, such as integrating advanced monitoring tools and improving internal compliance mechanisms.

The journey toward balancing compliance and confidentiality is fraught with challenges, yet banks are making strides by adopting advanced technology and strengthening global partnerships. While hurdles such as legacy systems, operational costs, and diverse regulations persist, proactive measures like blockchain adoption, AI-driven systems, and industry-wide collaborations underscore the sector's commitment to securing customer data while meeting regulatory requirements. These examples highlight the ongoing evolution of banking practices to navigate the delicate interplay between compliance and confidentiality effectively.

Conclusion

The KYC norms issued by the RBI highlight the critical balance between ensuring financial security and safeguarding customer privacy. These norms are fundamental to maintaining a crime-free banking environment while building trust in the financial system. However, with the rapid evolution of digital technologies and regulatory requirements, banks must continuously innovate and strengthen their data protection and compliance measures to reinforce the integrity of the financial system and also to maintain the trust and confidence of their customers, which is paramount in today's digital economy.

We trust you will find this an interesting read. For any queries or comments on this update, please feel free to contact us at insights@elp-in.com or write to our authors:

Mukesh Chand, Senior Counsel – Email – mukeshchand@elp-in.com

Disclaimer: The information contained in this document is intended for informational purposes only and does not constitute legal opinion or advice.

¹⁶ <https://www.livelaw.in/top-stories/supreme-court-agrees-to-hear-plea-alleging-data-privacy-violation-by-foreign-credit-information-companies-257546>

¹⁷ Jaiprakash Kulkarni vs The Banking Ombudsman Decided on 13 June, 2024- Bombay High Court

¹⁸ <https://www.fca.org.uk/news/press-releases/fca-fines-and-imposes-restriction-canara-bank-anti-money-laundering-systems-failings>